Deloitte.
University Press

New perspectives on how cyber risk can power performance

Cyber Risk

Risk powers performance.

Sam Balaji
Business Leader
Global Risk Advisory

The traditional view of risk management solely as a means of risk avoidance is changing. Perhaps, it's time to raise the possibility that risk is something we not only *should* accept, but embrace. This includes cyber risk. Reports of cyber breaches and attacks surface with alarming regularity. These reports tend to focus on the negative impacts of cyber risk: the data stolen, the value lost, and the damage done. This is understandable. Bad news makes good press. But shouldn't we acknowledge that cyber risk is an unavoidable part of doing business today? And shouldn't we expand our view of this risk to include opportunity?

The answer springs from the notion that risk powers performance. There is no reward without risk—and this, in a world where digital technology is vital to all aspects of business, is especially true of cyber risk.

Business leaders understand that doing what needs to be done to create enterprise value often means taking risks. Think about the range of initiatives that today's organizations undertake to pursue innovation, accelerate performance, and enable growth: Using social media tools to attract customers and to change how employees collaborate and engage. Outsourcing non-core activities to an array of often-distant suppliers and vendors. Applying exponential technologies like the Cloud and the Internet of Things to transform the business. All of these actions rely on communication and data management through digital technology. In fact, there's no escaping the reality that virtually everything an organization does, in this day and age, relies on digital technology—and thus is accompanied by at least some degree of cyber risk.

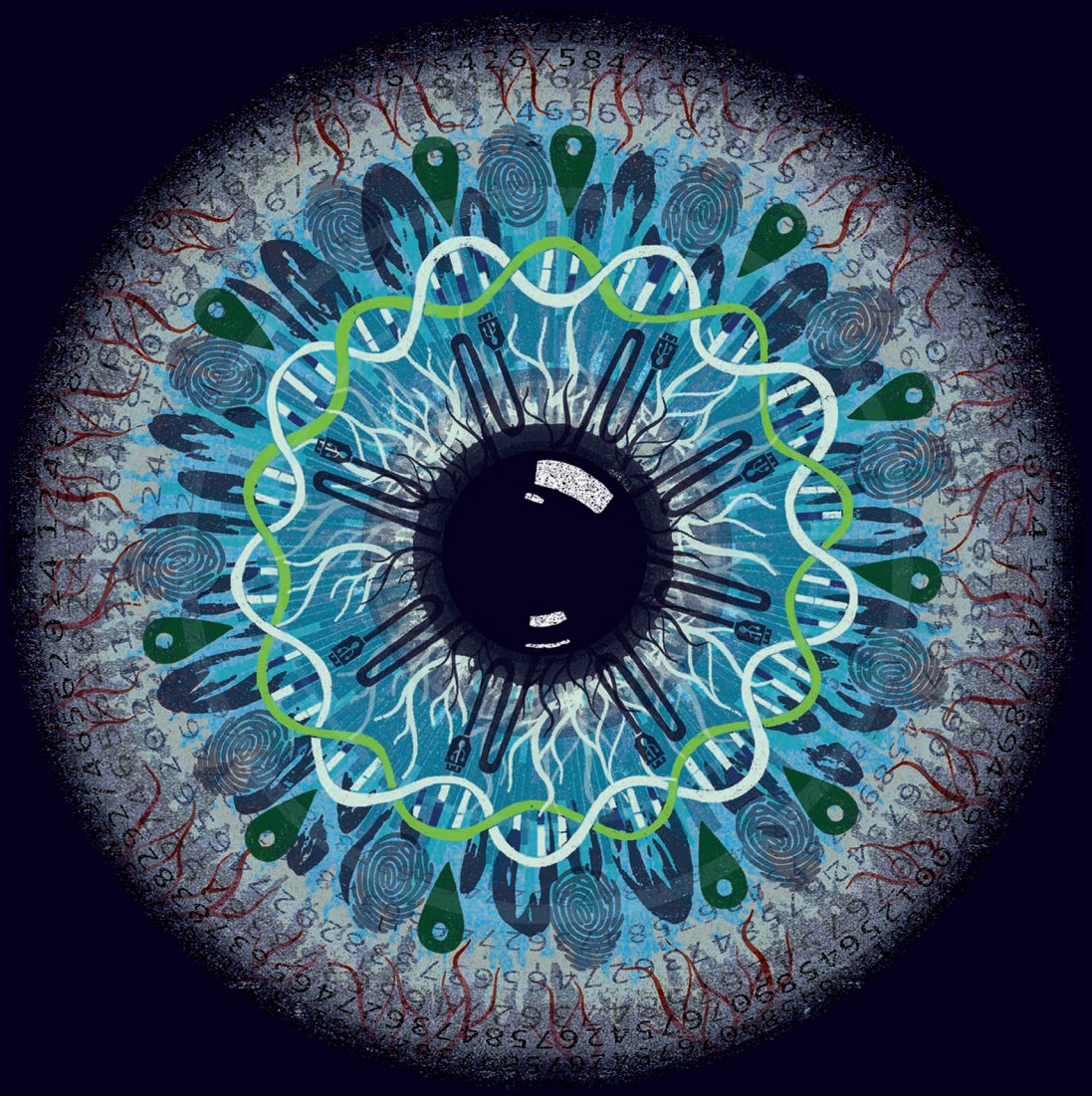
As with all risk, cyber risk must be managed with an eye to the organization's risk appetite. But when managed from the perspective that risk powers performance, cyber risk begins to take on a different flavor. Far from always being undesirable, it emerges as a thing to be consciously taken, an inevitable concomitant of growth. Leadership's task is to enter into situations that entail cyber risk with their eyes wide open so that understanding the risk, they can take steps to address it.

I encourage you to read the articles in this collection and use them to further conversations in your own organization about leveraging cyber risk to power performance.

Sam Balaji
Business Leader
Global Risk Advisory

CONTENTS

Artwork by Lucy Rose



A world beyond passwords

Improving security, efficiency, and user experience in digital transformation

By Mike Wyatt, Irfan Saif, and David Mapgaonkar

The next time you're at your computer about to access sensitive financial information about, say, an acquisition, imagine if you didn't have to begin by remembering the password you created weeks ago for this particular site: capitals, lowercase, numerals, special characters, and so on. Instead of demanding that you type in a username and password, the site asks where you had lunch yesterday; at the same time, your smart watch validates your unique heart-rate signature. The process not only provides a better user experience—it is more secure. Using unique information about you, this approach is more capable and robust than a password system of discerning how likely it is that you are who you claim to be.

Digital transformation is a cornerstone of most enterprise strategies today, with user experience at the heart of the design philosophy driving that transformation. But most user experiences—for customers, business partners, frontline employees, and executives—begin with a transaction that's both annoying and, in terms of security, one of the weakest links. In fact, weak or stolen passwords are a root cause of more than three-quarters of corporate cyberattacks,[1] and as every reader likely knows, corporate cyber breaches often cost many millions of dollars in technology, legal, and public relations expenses—and much more after counting less tangible but more damaging hits to reputation or credit ratings, loss of contracts, and other costs.[2] Shoring up password vulnerability would likely significantly lower corporate cyber risk—not to mention boost user productivity, add the goodwill of grateful customers, and reduce the system administration expense of routinely managing employees' forgotten passwords and lockouts.

The good news, for CIOs as well as those weary of memorizing ever-longer passwords, is that new technologies—biometrics, user analytics, Internet of Things applications, and more—offer companies the opportunity to design a fresh paradigm based on bilateral trust, user experience, and improved system security. Successful execution can help both accelerate the business and differentiate it in the marketplace.

In fact, the ability to access digital information securely without the need of a username and password represents a long-overdue upgrade to work and life. Passwords lack the scalability required to offer users the full digital experience that they expect. Specifically, they lack the scalability to support the myriad of online applications being used today, and they do not offer the smoothness of user experience that users have increasingly come to expect and demand. Inevitably, beleaguered users ignore recommendations[3] and use the same password over and over, compounding the vulnerability of every system they enter. Perhaps even more important, passwords lack the scalability to provide an authentication response that is tailored to the transaction value; in other words, strong password systems that require unwieldy policies on character use and password length leave system administrators unable to assess the strength of any given password. Without such knowledge, enterprises struggle to make informed risk-based decisions on how to layer passwords with other authentication factors.

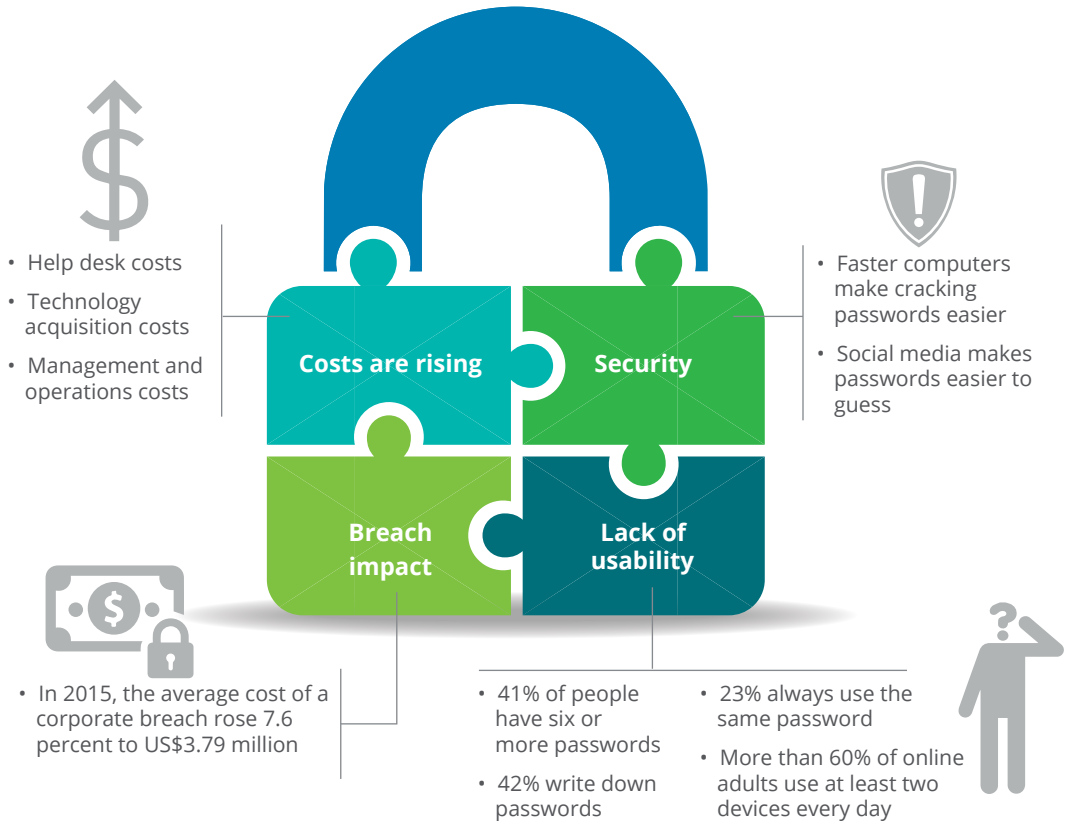
THE 21ST CENTURY MEETS HUMAN LIMITS

TWENTY years ago, a typical consumer had only one password, for email, and it was likely the same four-digit number as his or her bank account PIN. Today, online users create a new account every few days, it seems, each requiring a complex password: to access corporate information, purchase socks, pay utility bills, check investments, register

to run a 10K, or simply log into a work email system. By 2020, some predict, each user will have 200 online accounts, each requiring a unique password.[4] According to a recent survey, 46 percent of respondents already have 10 or more passwords.[5]

And the demands of password security are running into the limits of human capabilities, as shown in figure 1. According to psychologist George Miller, humans are best at remembering numbers of seven digits, plus or minus two.[6] In an era where an eight-character password would take a high-powered attacker 77 days to crack, a policy requiring a password change every 90 days would mean a nine-character password would be sufficiently safe.[7]

Figure 1. Why passwords are problematic



Sources: RoboForm, "Password security survey results—part 1," http://www.roboform.com/blog/password-security-survey-results, accessed April 21, 2016; Philip Inglesant and M. Angela Sasse, "The true cost of unusable password policies: Password use in the wild," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010): pp. 383–392; PortalGuard, *Top 10 real costs associated with requiring multiple passwords*, 2011; Tom Rizzo, "The hidden costs of passwords," *ScorpionSoft*, August 20, 2015, http://insights.scorpionsoft.com/the-hidden-costs-of-passwords; Victoria Woollaston, "Think you have a strong password? Hackers crack 16-character passwords in less than an HOUR," *Daily Mail*, May 28, 2013; Matt Smith, "The 5 most common tactics used to hack passwords," *makeuseof*, December 20, 2011, http://www.makeuseof.com/tag/5-common-tactics-hack-passwords/; Ponemon Institute, *2015 cost of data breach study: Global analysis*, May 2015; Olly Robinson, "Finding simplicity in a multi-device world," *GfK Insights Blog*, March 6, 2014, http://blog.gfk.com/2014/03/finding-simplicity-in-a-multi-device-world/.

Graphic: Deloitte University Press | dupress.deloitte.com

But such a long password—especially when it's one of many and changes regularly—starts straining people's memory. The inevitable result: People reuse the same weak passwords for multiple accounts, affix sticky notes to their computer monitors, share passwords, and frequently lean on sites' forgotten-password function. In a recent survey of US and UK users, 23 percent admitted to always using the same password, with 42 percent writing down passwords. While 74 percent log into six or more websites or applications a day, only 41 percent use six or more unique passwords.[8] According to another survey, more than 20 percent of users routinely share passwords, and 56 percent reuse passwords across personal and corporate accounts.[9] Password management software partially alleviates this particular issue, but it is still ultimately tied to the password construct.[10]

Even if an employee follows all regulations and has six distinct strong passwords that they remember, they still may be vulnerable. Humans can still be bugged or tricked into revealing their passwords. There is malware, or malicious software installed on computers; there is phishing, in which cyber crooks grab login, credit card, and other data in the guise of legitimate-seeming websites or apps; and there are even "zero day" attacks, in which hackers exploit overlooked software vulnerabilities.[11] And of course, old-fashioned human attacks persist, including shoulder-surfing to observe users typing in their passwords, dumpster-diving to find discarded password information, impersonating authority figures to extract passwords from subordinates, discerning information about the individual from social media sources to change their password, and employees selling corporate passwords.

No wonder the operational costs of maintaining passwords, including help-desk expenses for those who forget passwords, and productivity losses because of too-many-attempts lockouts and other issues are rising. Even more worrisome, ever-increasing computing power is enabling new brute-force attacks to simply guess passwords. The future of the password is both expensive and fraught.

- 74 percent of surveyed web users log into six or more websites or applications a day[12]
- 20 percent of surveyed employees routinely share passwords[13]
- 56 percent of surveyed employees reuse passwords across personal and corporate accounts[14]

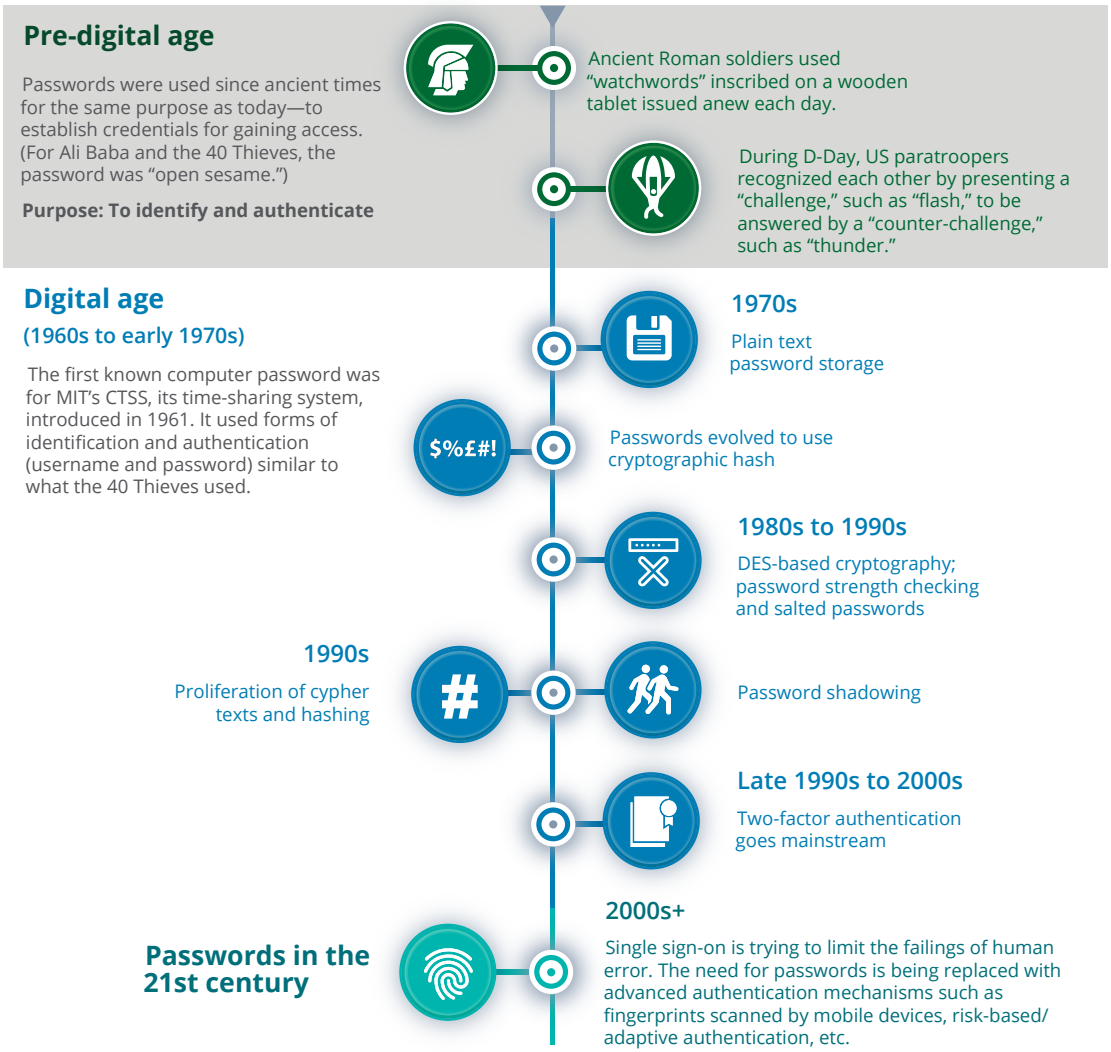
FROM GEOLOCATION TO BIOMETRICS

CORPORATE leaders are well aware that information and access strategy is at the core of nearly every business today. It's time to recognize also that the password—the mechanism used historically to implement this strategy—is fundamentally broken. Given their fiduciary and governance responsibilities, boards of directors and C-suite executives

FROM ANCIENT GREECE TO THE DIGITAL AGE

Passwords have been in use since ancient times for the same purpose as today: to establish one's credentials to access protected assets. Establishing authority in this way depends on presenting "something you know"—the password—to be "authenticated" against the registered value. As figure 2 shows, passwords have been a cornerstone of our history, including serving as a digital key for around the past 50 years. Indeed, digital passwords used to possess advantages: They were simple, easy to use, and relatively convenient. They could be changed, if compromised. Conveniently, they could be shared, though this practice compromises security. Because passwords are the prevailing standard, corporate policies governing them are well established, and identity and access management systems support them.

Figure 2. The password through history



Sources: Bryan Black, "The language of espionage: Signs, countersigns, and recognition," Imminent Threat Solutions, August 11, 2015; David Walden and Tom Van Vleck, eds., *The Compatible Time Sharing System (1961–1973): Fiftieth anniversary commemorative overview*, IEEE Computer Society, 2011; "Password security: Past, present, future," Openwall, 2012.

Graphic: Deloitte University Press | dupress.deloitte.com

owe it to stakeholders to guard the corporate treasure chest—digital information—by providing more robust online access protections. In turn, investors, customers, employees, partners, third-party vendors, and others will benefit from stronger protection of corporate data coupled with easier access for legitimate users, thus bolstering the bilateral trust that is at the heart of any healthy business relationship.

Increasingly, consumers, employees, and partners all expect seamless digital interactions, leading to a fundamental paradigm shift in how companies help conceive, use, and manage identities. Supporting the makeover, new login credentials might include not just "what you know" or a specific password but also "who you are" and "what you have," along with "where you are" and "what you are doing." They can include detection of personal patterns for accessing certain information by time of day and day of week, other dynamic and contextual evaluations of users' behavioral characteristics, individuals' geolocations, biometrics, and tokens. Systems that rely upon authentication are evolving to become adaptive and can flag an authentication attempt as being too risky if typical usage patterns are not met—even though basic credentials may appear correct—and the system can then step up authentication, challenging the user to provide additional proof to verify his or her identity. Because of its ubiquity, the mobile phone is the most obvious device over which authentication takes place, but venture capitalists are also funding companies creating other connected devices, such as wristbands that identify one's unique heartbeat and USB fobs that conduct machine-to-machine authentication without requiring a human to type in a passcode.[15]

Forces are converging for an overhaul. "From a technology perspective, we have amazing new authentication modalities besides passwords, and the computer capability to do the analysis to make informed decisions," says Ian Glazer, management council vice chair of the Identity Ecosystem Steering Group, a private sector-led group working with the federal government to promote more secure digital authentication. "We've also overcome one of the biggest challenges: We put the authenticator platform in everyone's hand in the form of a smartphone."[16]

For companies, navigating change from legacy to new systems is never easy. But by following a risk-based approach, they can create a well-considered roadmap to make the switch by focusing investment and implementation on the highest-priority business operations. Beginning with a pilot to test selected options, companies can then expand successful solutions to where they are needed most. Most of all, setting out on the road to change soon is crucial. After all, businesses are operating at a time when continued innovation and growth depend more than ever on the integrity of information.

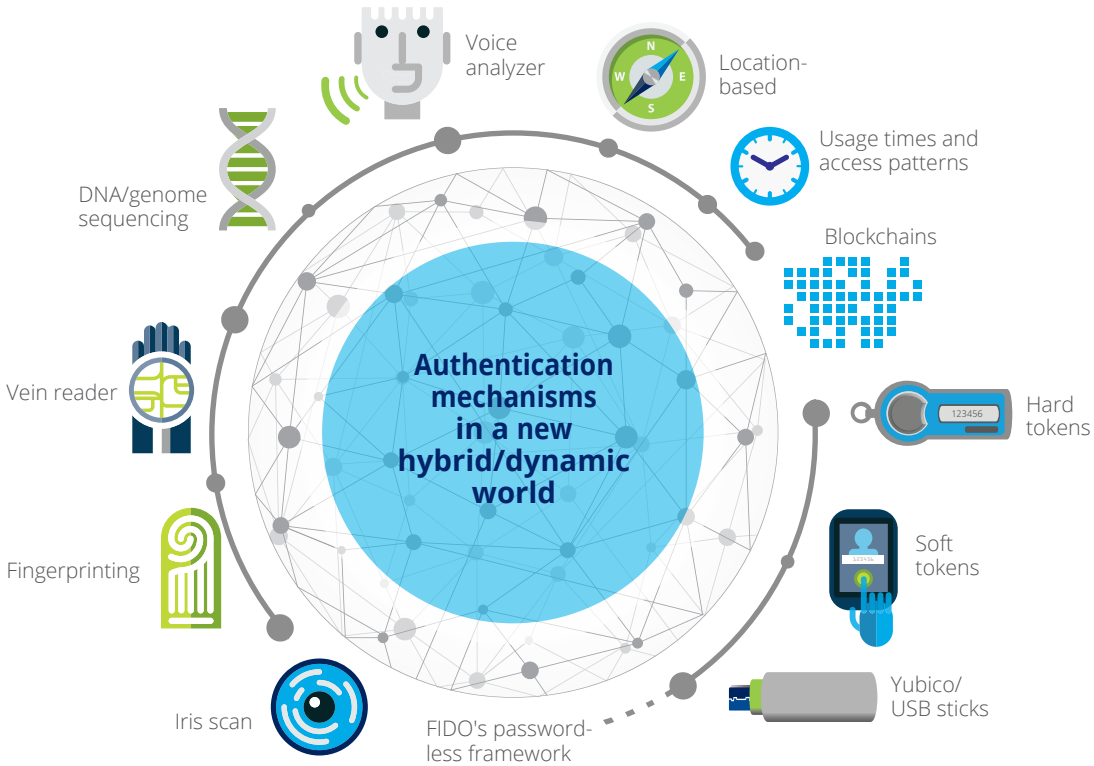
THE NEW GATEKEEPERS

WITH the costs of password protection—in time, risk, and dollars—mounting, enterprises are looking to implement flexible risk-based approaches: requiring user authentication at a strength that is commensurate with the value of the transaction being requested. Fortunately, as shown in figure 3, various technologies are emerging that can be combined in a way that satisfies enterprise risk tolerance and user flexibility at the same time. Emerging technologies such as blockchain[17] are positioned to replace the vulnerability of the single password with multiple factors.

Having multiple, cascaded gatekeepers fortifies security by requiring additional checkpoints. The more different proofs of identity required through separate routes, the more difficult it is for a thief to steal your identity or to impersonate you. Likewise, consumer platforms are paving the way by providing improved user experience by empowering consumers to choose how they access digital information.

The texting, sharing, and mobile-app economy has made immediate, seamless online

Figure 3. A new world with many gatekeepers



Graphic: Deloitte University Press | dupress.deloitte.com

communications and transactions ubiquitous. In a reversal of an earlier era, consumers are now the first adopters, followed by enterprises. Thus, as the smartphone becomes the consumers' digital hub, on their person almost at all times, it is well positioned to perform a central function. Already, the majority of 16-to-24-year-olds view security as an annoying extra step before making an online payment and believe that biometric security would be faster and easier than passwords.[18] Meeting these trends, leading technology companies founded the Fast IDentity Online Alliance in 2012 to advance new technical standards for new open, interoperable, and scalable online authentication systems without passwords.[19]

To maintain security and provide greater user convenience, a key precept in newly evolving login systems is *multi-factor authentication*. Gmail and Twitter, among others, today deploy this solution in simple form: They provide users a one-time code sent to their mobile phones to enter, in addition to the traditional password entered onto the user's laptop screen. Enhanced security comes from authentication taking place over two devices owned by the user. A cyber thief would have to have access to the user's phone, in addition to his or her online password, to get at the protected account.

For yet another layer of protection, in addition to delivery over different devices, the factors required for authentication can vary in type. In a two-factor authentication process, for example, a user could scan his or her retina via the camera on her laptop or smartphone, using biometric identification as a first step to gain access to his or her online bank account. In a second step, the bank could then send a challenge via text message to the user's mobile phone, requiring the user to reply with a text message to finish the authentication.

One of the most popular new factors for authentication is *biometric technologies*, which require no memorization of complex combinations of letters, numbers, and symbols, much less which combination you used for which resource.[20] It's simply part of you—your fingerprint, voice, face, heartbeat, and even characteristic movements. Biometrics that can be captured by smartphone cameras and voice recorders will likely become most prevalent first, including fingerprint, iris, voice, and face recognition. Checking your biometric data against a trusted device that only you own—as opposed to a central repository—is emerging as the preferred approach. For example, you could use your fingerprint to access a particular resource on your own smartphone, which in turn sends its own unique device signature to the authentication mechanism that grants you access.[21] This is the basis for scalability of authentication across multiple online services, and is the model that the Fast IDentity Online Alliance adopted.

A separate set of authentication factors come under the rubric of "what you have"—not only smartphones but perhaps security tokens carried by individuals, software-enabled

RISK-BASED AUTHORIZATION IN ACTION

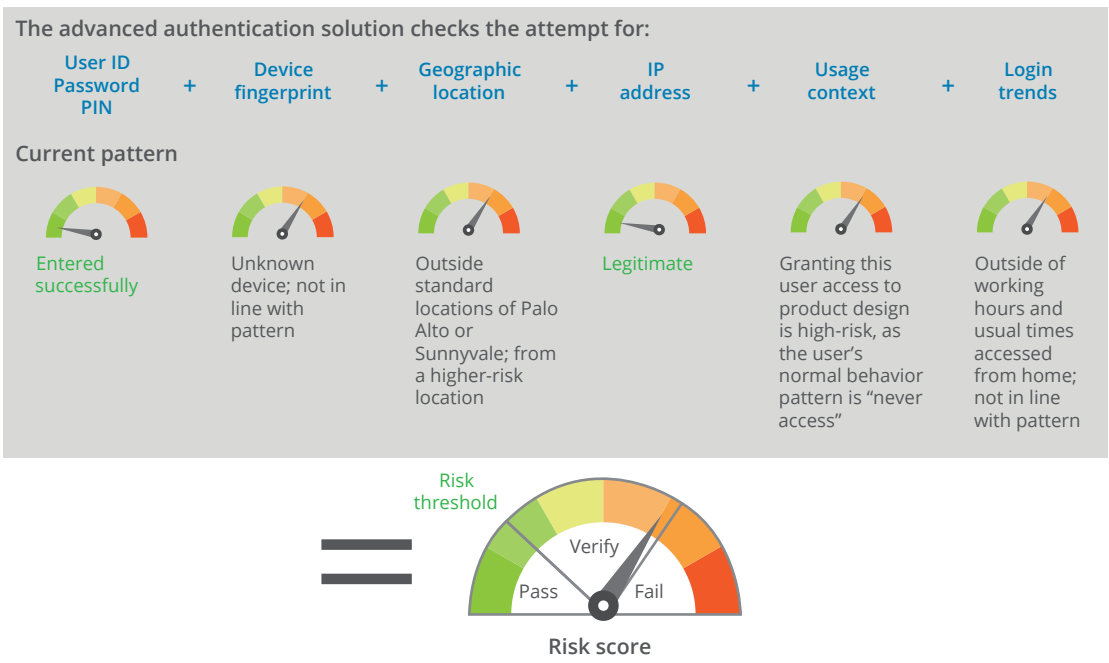
In a hypothetical example (figure 4), a corporate user usually logs in around 8:30 a.m. PST, logs out at 6 p.m., and logs in again around 9:30 p.m. Typically, he logs in from corporate offices in Palo Alto or Sunnyvale, accessing his company's systems during the day via a company laptop or desktop.

On Monday, the user tries to log in from his Sunnyvale office at 11 a.m., using a work computer to access the corporate finance system. The user is logging in from a company computer from his office during his regular hours for information he typically accesses. The system grants access.

The next day, the user attempts to log in from Los Angeles International Airport at 7 p.m., using a company laptop to access the list of company holidays on an internal benefits system. Though his location and time are unusual, the other factors are typical for him, and the information is not sensitive. The system grants access.

The following day, a hacker tries to log in from Belarus at 3 a.m. with the user's username and password to access designs for a not-yet-released company product on an internal development server. The username, password, and IP address are legitimate, but the other factors—such as location, time, and the information requested—are highly atypical for this user. The system implements controls that initiate step-up authentication techniques to verify the user's identity—for instance, sending a one-time authentication code to the user's phone. Because the hacker in this scenario does not have the user's phone, he or she is unable to enter the authentication code, and the system denies access.

Figure 4. Risk-based user authentication



Graphic: Deloitte University Press | dupress.deloitte.com

tokens, or even an adaptation of blockchain databases used by bitcoin. Hardware USB keys enable workers to login by entering their username and password, followed by a random passcode generated by the fob at set intervals of time. Software tokens operate similarly, with a smartphone app, for example, generating the codes. Further off, the potential use of distributed blockchain technology could help provide a more secure and decentralized system for authentication.

One of the most intriguing possibilities in new access controls is *risk-based authorization*, a dynamic system which grants access depending on the trustworthiness of the user requesting admission and the sensitivity of the information under protection. With Project Abacus, Google's Advanced Technology and Projects is developing machine learning to authenticate users based on multiple assessments of their behavior.[22] Using sensors such as the camera, accelerometer, and GPS functions, smartphones can gather a wide range of information about users, including typical facial expressions, their habitual geolocations, and how they type, walk, and talk. Together, these factors are 10 times safer than fingerprints and 100 times safer than four-digit PINs.[23] With such capabilities, a user's phone, or another device, can constantly calculate a trust score—a level of confidence—that the user is who he claims to be. If the system is in doubt, it would ask for more credentials through step-up authentication to verify the user's identity or deny access altogether.

Such trust-scoring is useful for designing protections for information, depending on its sensitivity. Banking apps, for instance, would require very high trust scores; access to general news sites might require less. For widespread adoption of this approach, companies must take consumer privacy issues into account.

THE BEST DEFENSE

TO illustrate how a company might adopt a new system, take the hypothetical scenario of a retail chain that discovers the theft of customers' credit card information. To fortify against future attack, the chain engages in a companywide assessment of its potential vulnerabilities and discovers three weaknesses that could have led to the attack: First, the server administration team keeps user names and passwords in an unencrypted text file on a shared directory. For convenience, store managers share their passwords for point-of-sale (POS) cash register systems with store associates to give them greater privileges to issue refunds, make exchanges, and the like. Last, to simplify integration, passwords for third-party vendors are set to never expire.

The retailer considers several new authentication options to strengthen security at points of sale, which analysis suggests were the most likely culprit in the breach. Managers decide against requiring employees to enter

a one-time password delivered by smartphone each time they want to access the system because of the inconvenience. Instead, they opt to test—in one division of stores—a combination of fingerprint and facial recognition to authenticate store associates' logins at POS systems. Not only is it more convenient for users, this option leverages existing infrastructure. Using cameras already in place to monitor POS activity, combined with a fingerprint-scanning application added to the login screen of touchscreen POS hardware, the company launches the pilot without additional hardware, spending primarily for third-party software development costs. The results: Store associates appreciate easier, faster logins; the company enforces the rights appropriate to a given user; and the constant reminder of the POS camera helps reduce theft among associates.

With the pilot's success, the retailer implements the solution across all 1,500 stores, updating policies to further ensure security for the new system, including the application of fingerprint and facial authentication to higher-security operations with greater impact and safe recovery mechanisms for compromised authentication factors.

The company also engages in educational outreach to store associates. Local store trainers emphasize the new system's ease of use, its effectiveness against vulnerabilities behind the original cyber theft, and the company's willingness to invest in the latest technologies for the benefit of employees and customers. In addition, trainers share documents explaining how the solution works, with strong assurances that the biometric information captured will not be used for purposes other than POS authentication.

NOT ONLY SECURITY—DIGITAL TRANSFORMATION

MOVING beyond passwords is not just a wave of the future—it makes economic sense today. A recent survey of US companies found that each employee loses, on average, US$420 annually grappling with passwords.[24] With 37 percent of those surveyed resetting their password more than 50 times per year, the losses in productivity alone can be staggering.[25] When you factor in the cost of the support staff and help desks required, the savings from eliminating passwords alone—let alone the security advantages—may begin to more rapidly justify a transition. Plus, streamlining employees' everyday tasks may improve employee happiness and productivity: Research into complaint departments in the United Kingdom found a correlation between process improvement and employee attitude and retention, and even variables as far afield as financial performance of the organization.[26]

True, abandoning a legacy password system—familiar, however irritating—and adopting new login methods may seem daunting for administrators, users, and customers. Any such migration requires a clear-eyed investment and implementation plan, aimed at overcoming very real challenges. First, from a technical

perspective, no system is airtight. If smartphones or tokens are a linchpin, lost or stolen devices could introduce risk: As in the case of a lost credit card, a user would have to contact the issuer of the device or authentication authority to report the loss and get a replacement. Crooks sometimes use account recovery of lost authentication factors to hijack accounts.[27] And mobile phones can be a weak link, since wireless communications are often unencrypted and can be stolen in transit.[28]

Even biometric technologies are not failsafe—many are difficult to spoof but are not spoof-proof. Fingerprints, for instance, can be faked using modeling clay.[29] System designers can address these potential vulnerabilities by implementing liveliness detection on sensors and storing the biometric information in an application-specific way, but these techniques are not ready to be fully implemented. Neither are most analytics-based systems, which won't deliver a full slate of benefits without business process changes. For example, consider the reputation-based security system discussed in the sidebar "Risk-based authorization in action." There, defenses examined not just the user ID attempting to access the system but also his location, time, behavior patterns, and the data he wished to access; in cases where these markers were unusual, the system denied access to sensitive business data. This is an excellent security approach but is predicated on an organization knowing and controlling all of its data: You can be aware if someone is trying to access sensitive data only if you have already classified that information as sensitive and determined its protocols for access.

Granted, moving beyond passwords may sound daunting, requiring major IT upgrades as well as changes to internal knowledge management and other business processes. But organizations can take incremental steps (figure 5) on the path toward a smooth transition. The following provides a roadmap:

- **Prioritize.** Assess strategic business priorities against the threat landscape and identify weaknesses in authentication systems for key business operations ranked by importance.

- **Investigate.** Examine possible solutions for stronger authentication, evaluating advantages and disadvantages in protecting against top threats and the ability to provide a practical, cost-effective, and scalable answer for the specific work environment. Standards-based authentication software solutions help to avoid the costs of new infrastructure and also to lay the groundwork for integration of next-generation solutions.

- **Test drive.** After choosing a promising solution(s), conduct a pilot in one or a few high-priority business operations. In these trials, collect data and feedback on users' experience. Are users able to adopt the solutions easily and intuitively? Has easier

Figure 5. Five things executives can do now

Graphic: Deloitte University Press | dupress.deloitte.com

online access made their work more efficient? Is online access then being used correctly more often in a way that provides greater security? Do users raise privacy or other concerns about any biometrics or adaptive, dynamic solutions based on their behavioral norms? From the online administrator's perspective, what is the experience in the costs of maintaining the new system, compared with the old password system?

- **Expand.** Harnessing lessons from the pilot, apply the solution to a wider swath of key operations in phases based on prioritization.

- **Revamp and educate.** Update access policies. Replace policies on password security with risk-based policies for authentication based on the sensitivity of information requested. Teach users how the new system works, focusing on its advantages over the old technology.

Technological advances are giving organizations the opportunity to begin moving beyond passwords—and they should strongly consider taking that opportunity, especially as cyberthreats expand. Given password mechanisms' poor user experience, rising costs, and security weaknesses, companies should look into migrating to new digital authentication systems that meet the twin objectives of tightening protection and improving user experience.

Organizations can begin their journey by starting to invest in non-password-based authentication solutions now as part of their digital transformation efforts, such as the rapid adoption of software-as-a-service platforms and omnichannel customer engagement initiatives. These new solution areas can serve as the foundation for broader enterprise authentication initiatives, which may take time. While we may have to live with passwords for some time given legacy platform constraints and technology limitations, there is no reason to delay the integration of non-password authentication initiatives.

Mike Wyatt *is a managing director with Deloitte & Touche LLP's Cyber Risk Services practice, where he leads digital and enterprise identity solution services for Deloitte's Advisory practice.*

Irfan Saif *is a principal in Deloitte & Touche LLP's Cyber Risk Services practice. He serves as the US Advisory Technology sector leader and is also a leader of Deloitte's CIO program and Cyber Risk practice.*

David Mapgaonkar *is a principal in Deloitte & Touche LLP's Cyber Risk Services practice, specializing in identity and access management.*

The authors would like to thank ***Abhi Goel***, ***Colin Soutar***, *and* ***Ian Glazer*** *for their significant contributions to this article.*

Endnotes

1. LaunchKey, *The decentralized authentication and authorization platform for the post-password era*, May 2015, https://launchkey.com/white-paper.
2. For more on the hidden costs of cyberattacks, particularly with regard to intellectual property, see Emily Mossburg, J. Donald Fancher, and John Gelinne, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," *Deloitte Review* 19, July 2016, http://dupress.com/articles/loss-of-intellectual-property-ip-breach.
3. Brian X. Chen, "Apps to manage passwords so they are harder to crack than 'password,'" *New York Times*, January 20, 2016, www.nytimes.com/2016/01/21/technology/personaltech/apps-to-manage-passwords-so-they-are-harder-to-crack-than-password.html.
4. Guillaume Desnoës, "How will we manage 200 passwords in 2020?," *ITProPortal*, September 13, 2015, www.itproportal.com/2015/09/13/how-will-we-manage-200-passwords-in-2020/; Steve Cook, "Could biometric give us a world without passwords?," LinkedIn Pulse, September 17, 2015, www.linkedin.com/pulse/could-biometrics-give-us-world-without-passwords-steve-cook.
5. Ian Barker, "84 percent of people support eliminating passwords," *BetaNews*, October 2015, http://betanews.com/2015/08/27/84-percent-of-people-support-eliminating-passwords/.
6. Hossein Bidgolli, editor, *Handbook of Information Security* (Hoboken, NJ: John Wiley & Sons, 2006), p. 434.
7. Ibid, p. 433.

8. RoboForm, "Password security survey results," www.roboform.com/blog/password-security-survey-results, accessed April 5, 2016.

9. Rob Waugh, "What are the alternatives to passwords?," *WeLiveSecurity*, February 5, 2015, www.welivesecurity.com/2015/02/05/alternatives-passwords/.

10. Chris Hoffman, "Why you should use a password manager and how to get started," *How-To Geek*, September 9, 2015, www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/.

11. Kim Zetter, "Hacking team's leak helped researchers hunt down a zero-day," *Wired*, January 13, 2016, www.wired.com/2016/01/hacking-team-leak-helps-kaspersky-researchers-find-zero-day-exploit/.

12. RoboForm, "Password security survey results—part 1," http://www.roboform.com/blog/password-security-survey-results, accessed April 21, 2016.

13. Kevin Cunningham, "Password management problems: Employees significantly increasing risk of security breaches," SailPoint, January 29, 2015, http://www.sailpoint.com/blog/2015/01/survey-password-management/.

14. Ibid.

15. Jeremy Quittner, "Why the 'Internet of Things' nabbed $1 billion in VC in 2013," *Inc.*, March 20, 2014, www.inc.com/jeremy-quittner/venture-capital-flows-to-gadget-and-hardware.html; Chris Quintero, "Who invests in hardware startups?," *TechCrunch*, September 12, 2015, http://techcrunch.com/2015/09/12/who-invests-in-hardware-startups/.

16. Ian Glazer, interview with Mike Wyatt, February 10, 2016, in Austin, TX.

17. See David Schatsky and Craig Muraskin, *Beyond bitcoin: Blockchain is coming to disrupt your industry*, Deloitte University Press, December 7, 2015, http://dupress.com/articles/trends-blockchain-bitcoin-security-transparency/.

18. Visa Europe, "Generation Z ready for biometric security to replace passwords," January 12, 2015, www.visaeurope.com/newsroom/news/generation-z-ready-for-biometric-security-to-replace-passwords.

19. FIDO Alliance, "About the FIDO Alliance," https://fidoalliance.org/about/overview/, accessed April 5, 2016.

20. PYMNTS.com, "Is it time to cash in PINs for biometrics?," January 28, 2016, www.pymnts.com/news/biometrics/2016/is-it-time-to-cash-in-pins-for-biometrics/.

21. Mark Hachman, "Microsoft's Windows Hello will let you log in to Windows 10 with your face, finger, or eye," *PCWorld*, March 17, 2015, www.pcworld.com/article/2898092/microsofts-windows-hello-will-let-you-log-in-to-windows-10-with-your-face-finger-or-eye.html; Hachman, "Hands on: Without apps, Intel's RealSense camera is a puzzle," *PCWorld*, March 5, 2015, www.pcworld.com/article/2893270/hands-on-without-apps-intels-realsense-camera-is-a-puzzle.html.

22. Beverly Zena Janelinao, "Project Abacus: Google's plan to get rid of the password," *Travelers Today*, January 25, 2016, www.travelerstoday.com/articles/21353/20160125/project-abacus-google-s-plan-to-get-rid-of-the-password.htm.

23. Tom Maxwell, "Smart Lock Passwords is cool, but Google Project Abacus puts us closer to a password-free world," 9to5Google, May 29, 2015, http://9to5google.com/2015/05/29/smart-lock-passwords-is-cool-but-google-project-abacus-wants-to-eliminate-password-authentication/.

24. Centrify, "U.S. businesses lose more than $200,000 annually from employees struggling with passwords," October 14, 2014, www.centrify.com/about-us/news/press-releases/2014/us-businesses-lose-more-than-200-000-annually-from-employees-struggling-with-passwords/.

25. Ibid.

26. Robert Johnston, "Linking complaint management to profit." *International Journal of Service Industry Management* 12, no. 1 (2001): pp. 60–69 (2001).

27. Maya Kamath, "Hackers are using password recovery scam to trick victims into handing over their email account access," *TechWorm*, June 21, 2015, www.techworm.net/2015/06/hackers-are-using-password-recovery-scam-to-trick-victims-into-handing-over-their-email-account-access.html.

28. IBM MaaS60, *Mobile: The new hackers' playground,* Data Breach Today, February 6, 2016, www.databreachtoday.com/whitepapers/mobile-new-hackers-playground-w-2243.

29. Archibald Preuschat, "Watch out, your fingerprint can be spoofed, too," *Wall Street Journal*, February 24, 2016, http://blogs.wsj.com/digits/2016/02/24/watch-out-your-fingerprint-can-be-spoofed-too/?mod=ST1.


CISO

The new CISO

Leading the strategic security organization

By Taryn Aguas, Khalid Kark, and Monique François

Monitoring, repelling, and responding to cyberthreats while meeting compliance requirements are well-established duties of chief information security officers (CISOs), or their equivalents, and their teams. But the business landscape is rapidly evolving. An often-cited statistic holds that "90 percent of the world's data was generated over the last two years."[1] This explosion of connectivity provides companies new opportunities for customer growth and product development—but these opportunities come with a catch: As customer data, intellectual property, and brand equity evolve, they become new targets for information theft, directly impacting shareholder value and business performance. In response, business leaders need CISOs to take a stronger and more strategic leadership role. Inherent to this new role is the imperative to move beyond the role of compliance monitors and enforcers to integrate better with the business, manage information risks more strategically, and work toward a culture of shared cyber risk ownership across the enterprise.

Paradoxically, though CEOs and other C-suite executives may very well like the CISO's role expanded, these same executives may unknowingly impede organizational progress. While senior executives may claim to understand the need for cybersecurity, their support for the information security organization, and sometimes specific cybersecurity measures, can be hard to come by. For instance, 70 percent of executives are confident about their current security solutions, even though only 50 percent of information technology (IT) professionals share this sentiment.[2] So what's creating this organizational disconnect?

CISOs recognize they can benefit from new skills, greater focus on strategy, and greater executive interaction, but many are spinning their wheels in their attempts to get these initiatives rolling. Through insights uncovered from Deloitte's[3] CISO Lab sessions[4] and secondary research, we explore what barriers CISOs most commonly face when building a more proactive and business-aligned security organization, and describe steps they can take to become strategic contributors to the organization.

RECOGNIZE THE WARNING SIGNS

If executives and IT professionals have conflicting views on the necessity to expand the CISO's organizational reach, it may be critical to assess the warning signs. The need to elevate the CISO's role within an organization can manifest in several ways:

Leadership and resource shortcomings. The security organization's leader may be a business or IT director who lacks formal security training, is perceived to be tactical and operational in approach, or spends most of his or her time on compliance activities rather than cyber risk management. The function may have a small budget in comparison to the industry, with limited resources and skill sets, or the security program may not be adequately defined and may lack established processes and controls.

A security breach. An actual breach where data or systems are compromised can be a sign of systemic issues, operational failures, and, potentially, a culture that does not value security. Compliance lapses, audit issues, and a lack of metrics and transparency can all be harbingers of potential security problems as well.

Inadequate alignment with the business. Business units may view security as a policeman rather than as a partner. CISOs and their teams that do not make an effort to understand and partner with the business leaders often become roadblocks to the business achieving its objectives, which leads to employees circumventing the security team and security measures.

Organizational structural issues. The security organizational structure may not be well defined or buried several layers down in IT. A recent survey conducted by Georgia Institute of Technology sheds light on this issue: Only

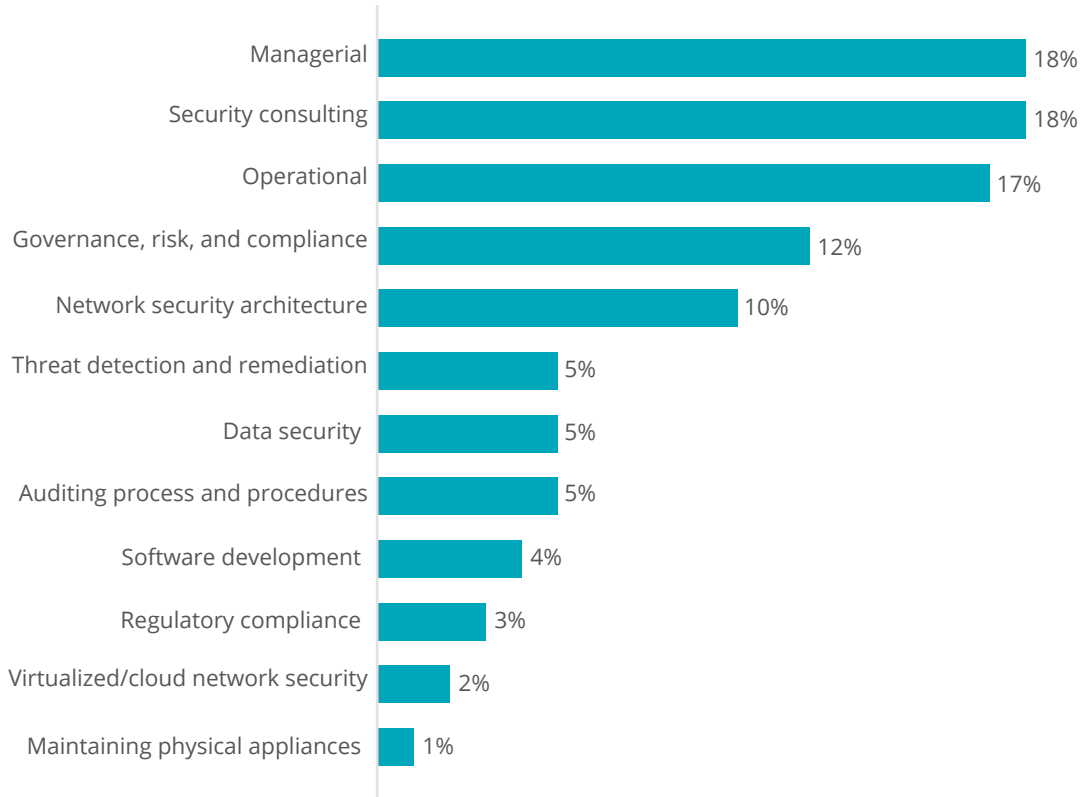
22 percent of respondents work in an organization where the CISO reports directly to the CEO, while 40 percent still report to the CIO.[5] And, whether housed in IT, risk management, legal, or operations, the security organization can be isolated from other areas of the business, impeding understanding and awareness of—as well as integration with—different functions.

Any of these signs can point toward a growing problem within an organization—one that simmers until a breach or other cybersecurity breakdown occurs, and the organization goes into crisis mode. This raises the question: Why isn't more progress being made?

CHALLENGES IN CREATING THE STRATEGIC SECURITY ORGANIZATION

WHY do companies struggle to strengthen cybersecurity? What factors are keeping CISOs from taking a more strategic enterprise role? The causes can lie within the security organization, in business units, and in communication between the two.

Figure 1. CISOs' former professional roles



Note: This figure shows the roles CISOs previously held before moving into the security organization.

Source: Frank Dickson and Michael Suby, *The 2015 (ISC)² global information security workforce study*, Frost & Sullivan, 2015, p. 36.

Graphic: Deloitte University Press | dupress.deloitte.com

Looking inward: When the CISO needs to look in the mirror

According to data from Deloitte's CISO Labs, building capabilities to better integrate with the business is a consistent priority among CISOs. Over 90 percent of CISOs hope to improve the strategic alignment between the security organization and the business, yet nearly half (46 percent) fear the inability to accomplish that alignment.[6] Why is that?

Narrow perspective. Because most are technologists by training and trade, CISOs typically have had limited exposure to and knowledge of the overall business. Before rising to management positions, many CISOs hold roles ranging from maintaining physical appliances and developing software, to compliance-related activities, threat detection/remediation, and network security architecture (figure 1).[7] If they don't receive management training that includes business and business development skills, this narrow perspective can impede CISOs' ability to view cyberthreats not simply as technical requirements but as critical risk issues—the latter a perspective vital to becoming a strategic player across the enterprise.

Communications and collaboration. CISOs can also struggle to communicate and collaborate with business leaders, in part because of limited interactions and relationships with them, a problem exacerbated by perceptions at the executive level. Most of Deloitte's CISO Labs participants (79 percent) reported they were "spending time with business leaders who think cyber risk is a technical problem or a compliance exercise." As a result, most CISOs "have to invest a lot of time to get buy-in and support for security initiatives."[8]

Those relationships are essential, though, in understanding what's happening in the business and where the greatest risks lie. For example, since it is virtually impossible to protect every piece of data in an organization, a security leader needs to work with the business to understand which data is critical to the enterprise, where it resides, and the impact should it be lost or compromised. Such exploration can suffer from a lack of clearly defined communication channels. Security doesn't have the tight integration and back and forth with the business enjoyed by functions such as customer service (which regularly provides information on customer demands and trends to other key functions) or finance (which delivers dollars-and-cents data to stakeholders across the organization).

Talent shortage. The lack of security talent can also keep the CISO from focusing on big-picture issues. The No. 1 reason CISOs stay mired in the weeds is because they have too few team members and not enough experienced talent.[9] Security is still a new skill set, one that is highly specialized and in high demand. According to a 2015 Frost & Sullivan survey, 62 percent of respondents said their organizations lack a sufficient number of security professionals, up from 56 percent just two years earlier. Furthermore, Frost & Sullivan predicts

"It's challenging to find people with the right skills, but the bigger problem is that it's a 'buyer's market.' Cyber professionals at almost every level have many options in front of them when deciding where to work. To be successful in attracting them, we have to make sure we convey the quality of our culture and the value of the contribution they can make."

—Genady Vishnevetsky, CISO, Stewart Title

that there will be a shortage of 1.5 million security professionals by 2020.[10]

Looking outward: The organizational climb of the CISO

Beyond issues specific to the CISO and team, security leaders also face headwinds from the broader business. Business program leaders often do not see the value of investing time and resources in understanding security beyond its more traditional functions. In contrast, they may be comfortably involved in other technology areas, such as the implementation of a customer relationship management (CRM) system, because they readily grasp the underlying business issues. Our research indicates two primary reasons for the lack of cyber risk focus at the organizational level: a false sense of security and competing agendas.

False sense of security. Many business-unit and C-suite executives think compliance equals security, especially in highly regulated industries. In Deloitte CISO Labs, 79 percent of CISOs report spending time with business leaders who think cyber risk is a technical problem or a compliance exercise.[11] However, being compliant with regulations does not address all cyber risk or make an organization secure, and that mind-set can create an organizational culture that has a very narrow and inadequate understanding of cyber risk.

Competing agendas. Business leaders have a role to play in elevating the importance of enterprise security, but it is a role many may view indifferently at best. A recent ThreatTrack survey revealed that 74 percent of C-suite executives do not think CISOs should have a seat at the table or be part of their organization's leadership team.[12] One reason may be that the mission of business units is to create new products and services, drive sales and revenue, and control costs in the process. Their results are not typically measured by, nor are they held accountable for, security considerations, and they don't readily make the connection between their strategic growth agenda and the cyber risks they tend to create.

STEPS TOWARD THE STRATEGIC SECURITY ORGANIZATION

CREATING a security organization that is a more strategic, integrated partner of the business requires both a new view of the CISO's role and a concerted effort to create a culture of shared ownership for cyber risk.

Elevating the CISO role

Increasing the value that the cyber risk program delivers to the enterprise requires a balanced approach. A successful CISO determines early on how to balance priorities and challenges across "four faces" of the CISO: *technologist*, *guardian*, *advisor*, and *strategist* (see the sidebar "The four faces of the CISO").[13] While all four roles are important, CISOs are being challenged to move beyond a traditional focus on the technologist and guardian roles. If their day-to-day actions and activities lean toward strategist and advisor, they are more likely to be viewed that way by other senior executives.

Assuming strategist and advisor traits

Today, much of a CISO's time and resources are spent managing and responding to threats. CISOs typically focus on activities such as overseeing and directing the implementation of security tools and technologies, identifying and blocking the leakage of digital assets, and managing the risk of and response to cyber incidents. The difficulty in differentiating between what is more and less important can lead to lumping security risks together and trying to protect the whole environment.

Moreover, a CISO's understanding of and appetite for risk may be quite different than that of a business unit leader. While the CISO may think in terms of reducing risks, business leaders take risks every day, whether introducing an existing product to a new market, taking on an external partner to pursue a new line of business, or engaging in a merger or acquisition. In fact, the ability to accept more risk can increase business opportunities, while ruling it out may lead to their loss. From this perspective, the role of the CISO becomes one of helping leadership and employees be aware of and understand cyber risks, and equipping them to make decisions based on that understanding. In some cases, the organization's innovation agenda may necessitate a more lenient view of security controls. Enabling business agility may require the CISO to lead more finely tuned efforts to detect threats early, and to emphasize preparedness for possible cyberattacks. (See "From security monitoring to cyber risk monitoring" in this issue for a more detailed discussion about how organizations can evolve toward a risk-focused threat monitoring program.)[14]

Change the conversation from security to risk (strategist role)

Taking on a more strategic role requires CISOs to pivot the conversation—both in terms of their mind-set as well as language—from

THE FOUR FACES OF THE CISO

CISOs continue to serve the vital functions of managing security technologies (technologist) and protecting enterprise assets (guardian). At the same time, they are increasingly expected to focus more on setting security strategy (strategist) and advising business leaders on security's importance (advisor). (See figure 2.)

Technologist. The CISO as technologist guides the design, development, and deployment of secure technical architectures, instilling security standards and implementing innovative countermeasures. Technologists carefully select and implement platforms that support changing threat detection and monitoring solutions, and integrate services delivered by external sources into a seamless framework. Technologists ensure that architecture designs are flexible and extendable to meet future security and business needs. They develop and maintain the security policies and standards that an organization should adhere to, working with the CIO to ensure that platforms meet these requirements.

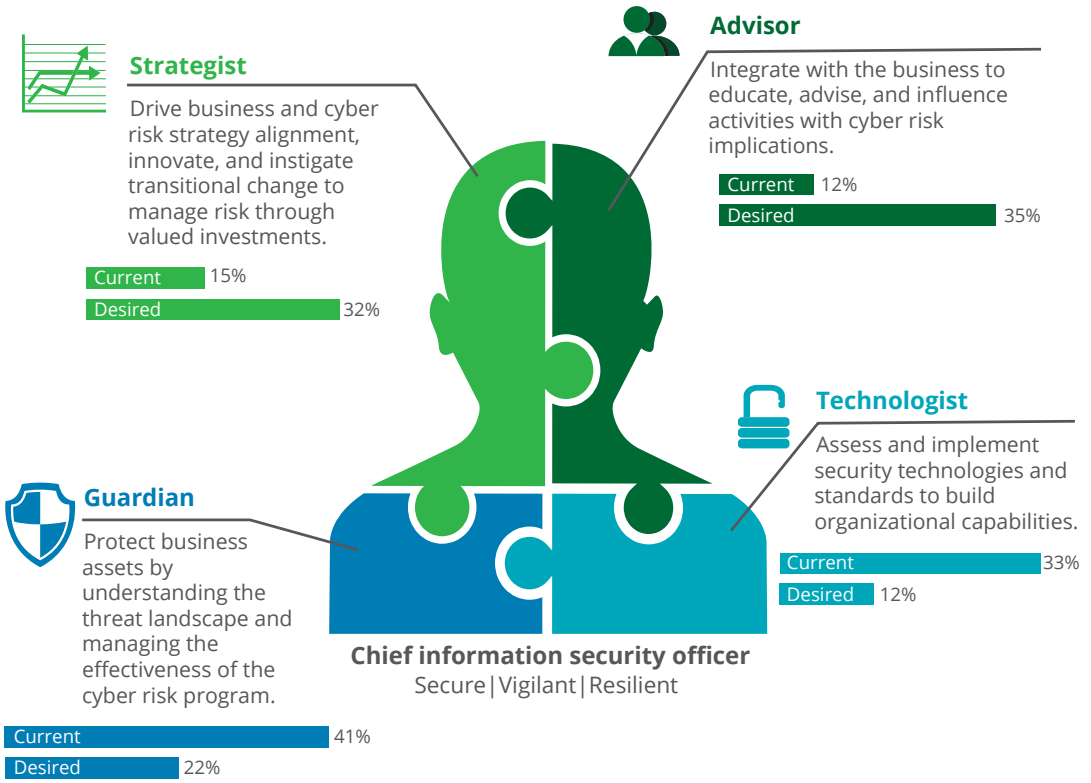
Guardian. As guardian, the CISO's charge is to monitor the effectiveness of the security program, processes, and controls in place. The guardian addresses considerations such as whether controls are working as intended, data is secure, and information is properly shared. Guardians monitor processes that safeguard the confidentiality, integrity, and availability of data and drive the overall security program. They also measure and report on information security risks to keep stakeholders informed and meet compliance and regulatory requirements.

Strategist. As strategist, the CISO is the chief value architect for all cyber risk investments. The strategist partners with the business to align business and information security strategies, and capture the value of security investments to safeguard enterprise assets. In this role, the CISO possesses deep business knowledge and acts as a credible partner who provides business-centric advice on how risk management can help the business. The strategist understands which business operations and information assets are the enterprise crown jewels, institutes strategic governance that prioritizes information security investments, and ensures that security and business resources and budgets are fully aligned to execute the priorities of the organization and deliver expected results.

Advisor. The CISO as advisor understands the implications of new or emerging threats, and helps identify cyber risks that arise as the business advances new strategies. The advisor drives the enterprise to continuously improve its security decision-making and risk mitigation capabilities. The advisor understands where the organization needs to focus to address cyberthreats, and creates a risk-based strategic roadmap to align cybersecurity efforts with corporate risk appetite. Advisors possess significant political capital and are able to enlist, educate, engage, and align executive stakeholders to increase security awareness.

security and compliance to focus more on risk strategy and management. Going beyond the negative aspect of how much damage or loss can result from risk, CISOs need to understand risk in terms of its potential to positively affect competitive advantage, business growth, and revenue expansion. For example, a CISO at a large retail organization used a three-tiered

Figure 2. The four faces of the CISO



Source: Research from Deloitte's CISO Transition Labs.

Graphic: Deloitte University Press | dupress.deloitte.com

risk model to present cyber risks to the board and discussed the mitigation plans for the most critical risks. He also updated the board on the risks business leaders decided to accept and why, including context on the business benefit.

Measure and report risk (strategist and advisor roles)

As the saying goes, what gets measured gets done. In cybersecurity, what gets measured gets noticed, so it is important for CISOs to define metrics that tell a story to which business leaders can relate. A CISO at a large technology company told a story about how he had run into his CEO in the hallway and told him that the team had blocked 125,000 malware attacks the previous month. The CEO's response was, "Isn't that your job?" The CISO acknowledged that he had blurted out the number without providing the right context.

To circumvent this issue, another CISO in a large financial services organization created a menu of security metrics, including acceptable upper and lower bounds for each metric, and then spent six months working with his

QUESTIONS TO SHAPE THE CYBER RISK ORGANIZATIONAL PROFILE

1. What are the key drivers of value in the organization, and how are these being protected?
2. What are the threats and vulnerabilities that provide the greatest exposure to us today?
3. To what extent do we have the foundational capabilities and practices in place to protect our critical assets?
4. How effective are we at monitoring and detecting cyber incidents?
5. Can we effectively respond to and recover from a cyber incident? Do we have response plans in place, and have they been tested?
6. What metrics demonstrate that we are effectively protecting the company?

stakeholders to create a custom cyber risk dashboard for each of their business areas. This helped the organization prioritize risk remediation as well as understand where risks may be acceptable.

In a report released by the World Economic Forum, cyber risk conversations should weigh three variables: the vulnerability of the system, the value of the assets at stake, and the sophistication of the attacker.[15] Bringing these three elements into the conversation highlights the relative importance of cyberthreats for business leaders. (To help facilitate these conversations, refer to the sidebar "Questions to shape the cyber risk organizational profile.") No longer is the conversation limited to issues of compliance; instead, business leaders can understand the costs of a threat that interrupts the business, as well as the likelihood of that event occurring in the current environment.

The CISOs who can align their risk metrics with the business's most pressing issues are more likely to be heard by strategic leadership. Making these insights easy to consume through intuitive dashboards can only help further solidify the CISOs' importance.

ADDRESSING TALENT DEMANDS

If CISOs hope to assume a more strategic role, they need to tackle organizational issues such as a shortage of security talent to support operational and technical activities—a key issue that can keep CISOs mired in minutiae. A recent Black Hat survey indicated that roughly 73 percent of organizations need more skilled security talent—a finding closely aligned with data from a Deloitte CISO Labs survey, which found that over 75 percent of participating CISOs noted a lack of skilled resources and effective team structure to support their priorities.[16]

To build upon organizational talent, CISOs should focus on developing a security-specific talent strategy that leverages existing skill sets, better integrates with stakeholders, and plans to fill the future talent pipeline.

Enhance the current workforce

The individuals you recruit or who are currently on your CISO team need to build their skill sets to accommodate the needs of the organization. One path organizations have taken is to cultivate relationships with technical institutes and universities to target specific skills needed, even establishing internship programs that focus on nurturing relationships with students and developing skills that align with the organization's goals and objectives. Another avenue of professional development comes from cyber risk "war games" training.[17] These are simulated scenarios designed to both test the readiness of an organization for specific cyber vulnerabilities as well as provide employees with hands-on experience for such events.

Integrate with the business

For fields outside of cybersecurity and risk, a number of studies have demonstrated that individuals with extensive "internal collaboration networks" routinely outperform those who work independently. These studies have been validated for fields such as engineering, research, and consulting.[18] In this spirit, it may be worthwhile for CISOs to focus on greater business collaboration that enhances the skill sets of both the cyber risk expert and the business leader.

The CISO may also consider developing an integration model by either designating cyber risk champions within business units or aligning cyber risk personnel with business units. Integrating talent resources can help employees understand where to go with security questions, and it can facilitate security professionals' understanding and awareness of business strategy and related cyber risk management requirements. The reality is that cybersecurity should be a priority for all employees. And, regardless of where the CISO function is positioned within the organization, it is important to understand where dotted-line relationships may exist and to clearly define roles to avoid confusion in responsibilities, and improve integration and collaboration.

Build future cyber risk leaders

In the longer term, it is important to consider both CISO succession planning and development of other leaders who can represent the CISO across the organization. Such candidates, manager level and up, need to be identified early and cross-trained, not just within security but across other areas of the business. Recently, George Washington University's School of Business has collaborated with the university's Center for Cyber and Homeland Security to offer a specialized "MBA with Cybersecurity" program to arm future organizational leaders with the "in-depth knowledge, resources, and network to drive global economics, innovation,

and policy" to meet the next generation of cyber challenges.[19] There are many other international programs with a similar focus, such as the MBA in Cybersecurity offered by Coventry University in the UK intended to enable graduates with the skills to "understand complex business problems and key issues in cyber security whilst exploring many associated business issues."

Such training can further build CISO candidates' credibility inside and outside the cyber risk function before they step into leadership roles, as well as help change the business perception that security professionals are purely technical and tactical.

LEADERSHIP EDUCATION, ENGAGEMENT, AND OWNERSHIP

HOW can CISOs secure executive support and involvement in encouraging cultural change and shared ownership of security across the enterprise?

Develop a communications strategy and plan

A CISO's communication plan should directly align with her or his vision and goals, and it should convey what success would look like for each functional area or executive role. Messaging should scale to all areas of the organization and be integrated with other business and functional messaging. Communications should highlight what is trending in security, both within the organization and in other similar businesses or government agencies. The discussion of those trends should be tailored so they are relevant to employees to help them understand the impact of the trend. Additional working tips and reminders about employee responsibility for keeping data safe can help drive the message home.

When communicating to the highest levels such as executive teams or boardrooms, make sure the messaging is on point and topical to the audience (see the sidebar "Communicating in the boardroom"). The plan should lay out how to establish conversations between leadership and the organization, whether through presentations, social media campaigns, or other means. This is an important step in setting the tone for broader culture change.

The goal is to clarify and justify a new view of risk and security, as well as inspire and catalyze employees to embrace it. One CISO hired two full-time media people on his team to spruce up his messaging and narrative to his leadership and to the rest of his organization.[20]

Enhance employee ownership by creating emotional connections

Studies from the fields of psychology, behavioral economics, and marketing have repeatedly shown that emotions rather than reason tend to drive human behavior. Because habits are tough to break with rational arguments alone, CISOs must inspire the business leaders who, in turn, must inspire employees to carry out the hard work of modifying their behavior and outlook.

COMMUNICATING IN THE BOARDROOM

Cyber risk is a business issue that board members may find especially challenging to oversee. In an effort to make the conversation more relevant and relatable, consider focusing your message on the following points:

- **Top cyber risks.** Tell the story of the current risk assessment results and the corresponding mitigation controls and management actions, particularly as they relate to top current business challenges.
- **Program maturity.** Explain your organization's maturity level in relation to the threat landscape and industry peers.
- **Emerging threats.** Identify who is attacking the company or its industry peers and the lessons learned. Explain news events and trends, such as the spread of ransomware or a high-profile data breach, and explain how they might impact your organization.
- **Audit and regulatory concerns.** Give status updates of any open audit and regulatory issues.
- **Public or private partnership.** Make note of any industry group participation and collaborations with law enforcement or intelligence agencies.

Many decisions the board wrestles with—whether related to new products, new markets, or mergers and acquisitions—are not directly about technology or security, but they have important cyber risk implications. A key objective for the CISO when interacting with the board is to become a trusted advisor who proactively helps illuminate these issues.

The Deloitte University Press article *Toeing the line: Improving security behavior in the information age* explains four behavioral elements that can modify organizational culture pertaining to risk practices:[21]

1. **Learning from policy.** Providing policies for employees to read is a natural first step. These are the artifacts that represent espoused values. However, policies alone will not sufficiently change behavior if the group does not act accordingly.

2. **Providing mentorship.** Social cues are a powerful influencer in determining what people value and how they should conform. Executives who embody new cybersecurity cultural attributes set a strong example for their direct reports and staff. When executives share their personal experiences in changing their own cybersecurity behaviors—and the challenges they've faced—they are more authentic, and their experiences can help other employees surmount similar hurdles.

3. **Group learning.** Draw from the work of consumer marketers in developing communications. For example, to foster more collaboration among employees, consider

having executives present examples of success stories from within the organization that highlight impactful cyber interventions at work.

4. **Learning from daily work.** Linking individual employees' day-to-day responsibilities to larger goals and to the organization's cyber resilience can give meaning to seemingly mundane activities. It can also lead to greater commitment and engagement. With more passionate employees, companies tend to derive greater productivity and profits.

These steps can help CISOs build credibility across the enterprise, fulfilling their role as advisor, and establish a work environment in which employees are empowered with security knowledge, requirements, and data to appropriately identify and mitigate risks on their own.

Table 1. Summary of CISO steps in the journey to a strategic security organization

Challenges	Steps to overcome them
Narrow perspectives	• Pivot the conversation from security to risk in order to facilitate more holistic conversations concerning the business • Stop viewing risk as categorically negative; calculated risks can lead to new business opportunities
Communication and collaboration	• Integrate with the business by developing cross-functional teams that include cyber risk specialists and business leaders • Borrow lessons from psychology and behavioral economics to create communications that speak to human behavior and thinking • Take advantage of a number of communication channels such as presentations, social media, and executive success stories
Talent shortage	• Explore partnerships with universities and professional organizations to enhance team skill sets • Leverage simulations and gaming scenarios to prep your team for high-risk events • Develop your "nontechnical" employees with leadership potential to be well versed in cyber risk
False sense of security	• Use dashboards to highlight current risk levels • Educate leadership on the difference between compliance and cyber risk management through communications and stories
Competing agendas	• Develop a stronger understanding of the business, and act as a strategist and advisor to the organization • Connect with leadership and the board to raise awareness; provide risk metrics that align with high-priority business efforts • Use communications and stories to create emotional connections that promote shared accountability

The importance of fostering an environment of security and risk awareness, shared ownership of cyber risk, and cyber risk resilience is only going to grow. CISOs who are able to step beyond a tactical, technical level are more likely to gain credibility and support among leaders across the enterprise, including the board, CxOs, and business unit leaders.

GAINING TRACTION, MOMENTUM, AND STRATEGIC DIRECTION

As cyber risks grow and evolve with technology advancement, so will the demands on CISOs, organization leaders, and employees. Instead of impeding innovation for fear of cyberthreats, the CISO should seek to be instrumental in aiding organizations to achieve their goals. The importance of fostering an environment of security and risk awareness, shared ownership of cyber risk, and cyber risk resilience is only going to grow. CISOs who are able to step beyond a tactical, technical level are more likely to gain credibility and support among leaders across the enterprise, including the board, CxOs, and business unit leaders. That is an important first step in leading efforts to create and sustain a culture of cyber risk awareness. Table 1 provides a summary of the other steps required to build a strategic security organization.

By earning a seat at the leadership table, helping imbue a shared sense of responsibility for cyber risk management, and providing guidance on how organizational leaders and employees can meet that responsibility, CISOs can become key drivers in the journey to the strategic security organization.

***Taryn Aguas**, a principal with Deloitte & Touche LLP, specializes in cybersecurity and technology risk management and leads Deloitte's CISO Lab program.*

***Khalid Kark** is a director with Deloitte Consulting LLP, where he leads the development of research and insights for the CIO Program.*

***Monique François** is a managing director with Deloitte Consulting LLP with over 20 years of experience guiding companies through complex change.*

Endnotes

1. "Big data, for better or worse: 90% of world's data generated over last two years," *Science Daily*, May 22, 2013, https://www.sciencedaily.com/releases/2013/05/130522085217.htm.

2. Barkly, *2016 cybersecurity confidence report*, http://cdn2.hubspot.net/hubfs/468115/Barkly_Cybersecurity_Confidence_Report.pdf, accessed April 11, 2016.

3. As used in this article, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

4. The Deloitte CISO Labs are immersive one-day workshops that encourage CISOs to think from a new perspective and develop a plan for success by focusing on the three most important resources a CISO has to manage: time, talent, and stakeholder relationships.

5. Jody R. Westby, *Governance of cybersecurity: 2015 report*, Georgia Tech Information Security Center, October 2, 2015, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf.

6. Deloitte CISO Labs data, 2015.

7. Frank Dickson and Michael Suby, *The 2015 (ISC)² global information security workforce study*, Frost & Sullivan, 2015, p. 3.

8. Deloitte CISO Labs data, 2015.

9. Ibid.

10. Dickson and Suby, *The 2015 (ISC)² global information security workforce study*, p. 36.

11. Deloitte CISO Labs data, 2015.

12. ThreatTrack Security Inc., *No respect: Chief information security officers misunderstood and underappreciated by their C-level peers*, June–July 2014, https://www.threattracksecurity.com/resources/white-papers/chief-information-security-officers-misunderstood.aspx.

13. Deloitte CISO Labs data, 2015. The "four faces of the CISO" concept is adapted from the framework presented in Ajit Kambil, *Navigating the four faces of a functional C-level executive*, Deloitte University Press, May 28, 2014, http://dupress.com/articles/crossing-chasm/.

14. Adnan Amjad, Mark Nicholson, Christopher Stevenson, and Andrew Douglas, "From security monitoring to cyber risk monitoring: Enabling business-aligned cybersecurity," *Deloitte Review* 19, July 2016, http://dupress.com/articles/future-of-cybersecurity-operations-management.

15. World Economic Forum in collaboration with Deloitte, *Partnering for cyber resilience: Towards the quantification of cyber threats*, January 2015, http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

16. Black Hat, *2015: Time to rethink enterprise IT security,* July 2015, https://www.blackhat.com/docs/us-15/2015-Black-Hat-Attendee-Survey.pdf; Deloitte CISO Labs data, 2015.

17. Cat Zakrzewski, "Cybersecurity training, military style," *Wall Street Journal*, March 13, 2016, http://www.wsj.com/articles/cybersecurity-training-military-style-1457921566.

18. Jim Guszcza, Josh Bersin, and Jeff Schwartz, "HR for humans: How behavioral economics can shape the human-centered redesign of HR," *Deloitte Review* 18, Deloitte University Press, January 25, 2016, http://dupress.com/articles/behavioral-economics-evidence-based-hr-management/.

19. George Washington University, "World executive MBA with cybersecurity," http://business.gwu.edu/programs/executive-education/world-executive-mba/, accessed April 12, 2016.

20. Deloitte CISO Labs data, 2015.

21. Joe Mariani et al., *Toeing the line: Improving security behavior in the information age*, Deloitte University Press, January 28, 2016, http://dupress.com/articles/improving-security-behavior-in-information-age-behavioral-economics/.


PROBABILITY
WEIGHT
LOW
HIGH

Quantifying RISK

What can cyber risk management learn from the financial services industry?

By JR Reagan, Ash Raghavan, and Adam Thomas

THE financial services industry is known for its sophisticated approaches to managing the risk associated with the financial instruments it sells. It's an industry imperative: No informed customer would invest with a financial services firm that lacked provisions for guarding against extensive losses. Among these approaches, one of the most widespread is the use of "fantastically complex mathematical models for measuring the risk in their various portfolios."[1] These models even allow firms to assign a dollar value to that risk—effectively allowing portfolio managers to quantify the risk their investments generate.

Today, many organizations are entering a new risk domain—cyber risk management—that exhibits many of the same characteristics as financial risk management in the financial services industry. While the comparison between the two may seem far-fetched at first, there are, in fact, a number of parallels that suggest that experiences in one domain can hold valuable lessons for the other. These parallels include:

- **Complexity.** For years, the financial services industry has used complex financial instruments where risks arise from the interaction of many disparate factors. In the cybersecurity context today, businesses are incurring increasing risks through their use of complicated computer system architectures and adoption of cloud computing, bring-your-own-device IT models, mobility, and other digital advancements. Just as with highly complex financial instruments, the intricacies of the interactions among risk factors can make it difficult to identify and assess relevant risks. While risk models and other quantitative metrics and qualitative sources can provide warning signs, business leaders in both the modern financial services and cyber risk eras face the distinct possibility that these warning signs may not always be clearly understood.

- **The use of models for risk management.** Financial institutions use a variety of risk models, some long established and others relatively new. Some risk management leaders today who attempt to apply quantitative models to measure cyber risk rely on some of those same types of models. The danger here is that senior executives and boards may overlook the complexity and, in some cases, limits of these models. The simplicity of many of these models' outputs—often a single, easy-to-fathom number—can mask the intricacy of the models' inputs and analysis process, potentially prompting executives to assume their quality and completeness rather than carefully scrutinizing the models' validity under particular circumstances.

- **Potential systemic failures.** In the financial services industry, there is constant recognition that financial institution failure can have ripple effects across borders, entire segments of the financial services industry, and, ultimately, much of the rest of the economy. Today's cyber risks potentially threaten entire ecosystems, including business, government, and societal.

Of course, public officials and leaders in many private sector industries are highly aware of cyber risks. Cybersecurity spending worldwide continues to grow, and is predicted to reach US$170 billion by 2020, up from US$75.4 billion in 2015.[2] Yet many struggle to determine the scope of those risks and how to appropriately balance risk-reward trade-offs.

It is this drive to quantify cyber risk and calculate the return on investment in cybersecurity that is fueling efforts to put a number to the extent of a company's cyber risk—paralleling the importance financial services firms place on quantifying financial risk. Investment, banking, and insurance executives understand that they take sometimes significant risks, and they want a number gleaned from risk models to quantify that risk and guide their decisions. However, in certain instances, the tantalizingly close potential for large rewards can lead executives to ignore the results of those models—or at least take them for granted by not fully grasping what the number really indicates.[3]

Similarly, business leaders today are confronted with the large demand for new technologies and the potentially huge returns from investing in these technologies. These leaders also understand, though, that by continuing to extend complex information systems and networks, they are often significantly increasing risk to the enterprise. This is leading to growing interest in developing risk models that quantify cyber risk and support the development and execution of cyber risk strategies and security programs.

What types of models are being used, and in what context? By relying too heavily on these models and ignoring other cyber risk indicators, could business leaders face a danger of being blindsided by a catastrophic cyber event?

Certainly, risk models are important tools for framing and understanding risk elements. But as they work to quantify cyber risk, enterprise leaders and chief information security officers can benefit from understanding financial institutions' risk management experience. Organizations should be cautious of relying solely on risk models and, instead, build strong governance processes surrounding these models. Without strong processes, leaders could become overconfident of their cyber risk posture—and oblivious to warning signs—leading to potential financial, operational, and reputational loss.

THE RISK OF A BLACK SWAN EVENT

VARIOUS types of risk can influence the value and performance of financial investments, generally categorized as credit, liquidity, market, and operational risk. *Value at risk*, or VaR, is prominent among the modeling techniques financial institutions

have used for decades to calculate the market risk within their investment portfolios. VaR is "a statistical technique [for] measur[ing] and quantify[ing] the level of financial risk within a firm or investment portfolio over a specific time frame."[4]

In its most common form, VaR measures portfolio risks over short periods of time, assuming "normal" market conditions. An investment manager whose portfolio shows a VaR of US$100 million one week, for example, has a 99 percent chance of not losing *more* than that amount from the portfolio the following week.[5] However, VaR typically cannot describe the 1 percent of the time that US$100 million will be the *least* that can be lost. This limitation means that VaR cannot measure the risk of a "black swan event"—a highly improbable occurrence with outsized impact—such as cascading home foreclosures and subprime mortgage losses.[6]

KEY TAKEAWAY Risk models like VaR serve a vital function, aggregating a variety of inputs and providing an indicator for decision makers to factor into their reasoning. An inherent shortcoming, however, is that the output is only as good as the input, and neither necessarily quantifies all risks.

GROWING CYBER CONCERNS AND THE DRIVE TO QUANTIFY CYBER RISK

HERE, it's important to understand public and private sector concerns about cyber black swan events and the emerging role of a "cyber VaR" model in quantifying cyber risk.

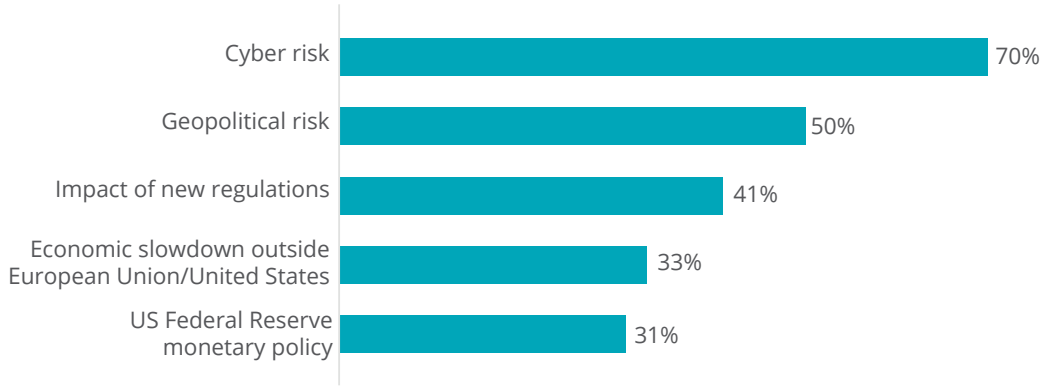
Officials across the globe are increasingly concerned about the risks that cyberthreats pose worldwide, some warning of the potential for cyber events to grow into systemic calamities. Greg Medcraft, former chairman of the board of the International Organization of Securities Commissions, for example, has predicted that "the next big financial shock—or 'black swan event'—will come from cyberspace, following a succession of attacks on financial players."[7]

Corporate risk managers also worry about a cyber black swan event. In a 2015 study by the Depository Trust & Clearing Corporation (DTCC), 61 percent of financial services risk managers surveyed believed the probability of a high-impact event in the global financial system had increased in the previous six months. As in the previous DTCC survey conducted in Q1 2015, cyber risk remained the No. 1 concern globally, with 70 percent of all respondents citing it as a top-five risk (figure 1). Respondents cited the frequency of attacks and the ability to manage them as top concerns.[8]

Certainly, cyberthreats are not exclusive to financial services and the global financial system. The potential for cyber black swan events in other sectors is a stark reality:

- **Utilities industry**. A December 2015 cyberattack that shut down part of Ukraine's power grid prompted the Obama administration to issue a warning to US

Figure 1. Top five risks to the global financial system



Source: The Depository Trust & Clearing Corporation, *Systemic risk barometer survey*, December 1, 2015.

Graphic: Deloitte University Press | dupress.deloitte.com

power companies, water suppliers, and transportation networks about the risk of similar attacks.[9]

- **Health care.** After persistent 2015 and 2016 cyberattacks on health care facilities and hospitals in North America, the US Department of Homeland Security, collaborating with the Canadian Cyber Incident Response Centre, issued a warning to health care organizations about ransomware and other variants that can cause "temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses," and reputational harm.[10]

- **Oil and gas.** Three out of four oil and gas, energy, and utility IT professionals surveyed in late 2015 had experienced an increase in successful cyberattacks, and most of those (68 percent) said the rate of successful cyberattacks had increased 20 percent in just the last month.[11]

- **Government.** A massive breach of the US Office of Personnel Management in 2014–2015 resulted in the theft of sensitive information, including the Social Security numbers of 21.5 million individuals from employee and contractor background investigation databases.[12]

So what actions are authorities and other stakeholders taking on a broad scale to respond to the growing systemic nature of cyberthreats?

One major initiative is the World Economic Forum's multi-stakeholder Partnering for Cyber Resilience initiative, launched at its 2011 annual meeting in Davos, Switzerland. Involving more than 100 experts, businesses, and policy leaders, the project's goal is to "address global systemic risks arising from the growing

digital connectivity of people, processes, and infrastructure."[13]

After first focusing on raising awareness of cyber resilience among senior-level leaders, in 2014 and 2015, the members shifted their attention to the need for "a shared cyber resilience assurance benchmark across industries and domains."[14] To create a successful risk quantification model, they began by listing various types of models used within their organizations. The Monte Carlo method was predominant, but elements of other models were also deemed important, including:

- Behavioral modeling
- Parametric modeling
- Baseline protection
- The Delphi method
- Certifications

The initiative's exploration led to the framing of a cyber VaR concept "based on the notion of value at risk, widely used in the financial services industry."[15] Using a probabilistic approach, a cyber VaR model estimates the likely loss an organization might experience from cyberattacks over a given period—that is, "Given a successful cyberattack, a company will lose not more than X amount of money over a period of time with 95 percent accuracy."[16]

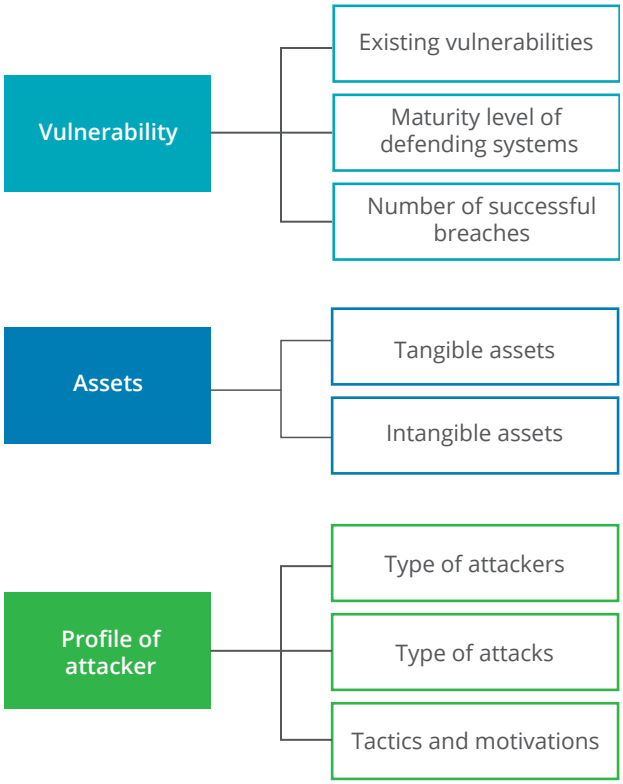
In explaining its decision to develop a measure based on financial VaR, the Partnering for Cyber Resilience initiative noted, "The financial service[s] industry has used sophisticated quantitative modeling for the past three decades and has a great deal of experience in achieving accurate and reliable risk quantification estimates. To quantify cyber resilience, stakeholders should learn from and adopt such approaches in order to increase awareness and reliability of cyberthreat measurements."[17]

The World Economic Forum stakeholders did not attempt to devise one specific cyber VaR model; instead, they suggested specific properties of a cyber VaR framework that industries and individual companies should incorporate into their own models. In this way, each organization can assess the components to determine applicability and impact to their own environment. That cyber VaR framework comprises these broad components (figure 2):

- *Vulnerability* of existing assets and systems and the maturity of defending systems
- *Assets* under threat, both tangible and intangible
- *Profile of attackers*, including types (for example, state-sponsored vs. amateur and level of sophistication) and their tactics and motivations

The cyber VaR components, some of which can represent random variables (variables subject

Figure 2. Cyber value-at-risk components



Source: World Economic Forum, *Partnering for cyber resilience: Towards the quantification of cyber threats*, January 2015.

Graphic: Deloitte University Press | dupress.deloitte.com

to "change due to chance," such as frequency of attacks, general security trends, and the maturity of an organization's security systems), are put into a stochastic model. The model is a statistical tool to estimate probability distribution incorporating one or more random variables over a period of time. Analysis of the dependencies between components can contribute to various models for estimating risk exposure.

Quantitative risk models represent an evolution in the management of cyber risk. However, when considering the cybersecurity realm, the use of risk models in general—and VaR specifically—invites an important question: Could a cyber VaR model pose a fundamental risk to organizations that choose to adopt it?

KEY TAKEAWAY The incredible complexity and ongoing expansion of the cyberthreat landscape are driving organizational initiatives to quantify cyber risk, much as financial institutions sought ways to quantify market risk in the burgeoning labyrinth of securities derivatives of the 1990s and early 2000s.

THE IMPORTANCE OF USING RISK MODELS—JUDICIOUSLY

THE answer to the question posed above hinges largely on the context within which an organization employs cyber VaR. We'll next explore how three very different approaches to using the VaR model yielded three diverse outcomes.

VaR's limitations were well known as far back as the 1990s, perhaps most famously in the 1998 fall of Long Term Capital Management (LTCM). LTCM's demise:

> Exposed the limitations of VaR modeling and inadequacies of historical probabilities in predicting the future. Because Russia defaulted on its domestic (rather than foreign) debt, something that had never occurred before, LTCM's VaR models assigned a probability of zero and incorrectly calculated the losses

of this event. The miscalculation threw LTCM into a liquidity crisis, eventually leading to a bailout by a private consortium of banks and financial institutions.[18]

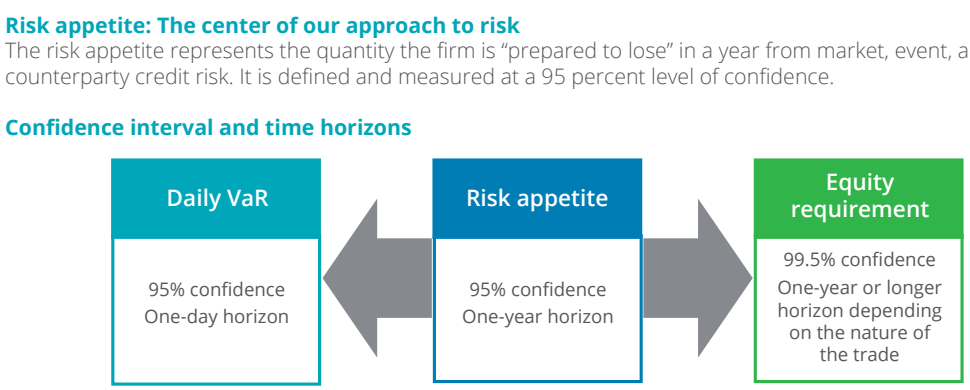
Despite this very public example of VaR's limitations, the model continued to be popular and widely used in the financial services industry. Different varieties of VaR were used by different firms, but, typically, a firm's stated risk approach involved daily VaR calculation at a 95 percent confidence level, as shown in figure 3.

The consequences of a laissez-faire attitude toward VaR outputs is illustrated by the experiences of a company we'll call Firm X, which had taken on an aggressive investment posture with the endorsement of its board of directors. According to emails from the risk management team, the firm's senior management disregarded its risk managers and failed to follow policies around its risk limits. Furthermore, management excluded certain risky principal investments from its stress tests without informing the board of directors, and it lacked a regular, systematic means of analyzing the amount of catastrophic loss that the firm could suffer from increasingly large, illiquid investments. And, in fact, Firm X eventually did suffer catastrophic losses that led to its bankruptcy.

Lessons learned in the years since Firm X's demise suggest the value of a different approach to corporate governance and risk management. This is illustrated by the story of another large financial firm, which we'll call Firm Y.

It starts when Firm Y leaders notice that the company's profit and loss figures reveal that its mortgage business has lost money for 10 consecutive days. Watching these trends closely, senior executives and risk managers decide to delve deeper to find out why this is happening. They examine the data thoroughly, and then choose to collaboratively examine the firm's trading positions.

Figure 3. Representative risk management integrated framework



Graphic: Deloitte University Press | dupress.deloitte.com

With a strong financial governance process in place, Firm Y uses a variety of quantitative risk measures—ensuring that none outweighs its profit and loss statements. Executives are careful to not rely solely on any one calculation or input source. By weighing all available evidence regularly and, using their professional judgment, Firm Y's leaders are likely to avert disaster by realizing they need to shed and hedge their mortgage-backed security positions.

How do the experiences of LTCM, Firm X, and Firm Y relate to quantification of cyber risk? One report points to shortcomings in board oversight of cybersecurity, concluding that boards are not paying close enough attention to security-related issues such as budgets, assessments, policies, roles and responsibilities, breaches, and even information technology risks.[19]

In describing the need for risk frameworks that address concerns about excessive reliance on risk models, José Manuel González-Páramo, an executive board member of a large global bank, said, "There has historically been an overreliance and mechanical use of models and external opinions. . . . Those models, measures, and opinions are still valid tools, but need to be used in a correct manner, and need to be complemented by other tools and, more generally, by expert judgment."[20]

Viewed in this context, the effective use of cyber VaR and other models to quantify cyber risk

One outcome of the Partnering for Cyber Resilience initiative is for participants to collaborate on devising an approach to "near-real-time information sharing [that] can address data availability challenges and supply enough data to build statistical models."

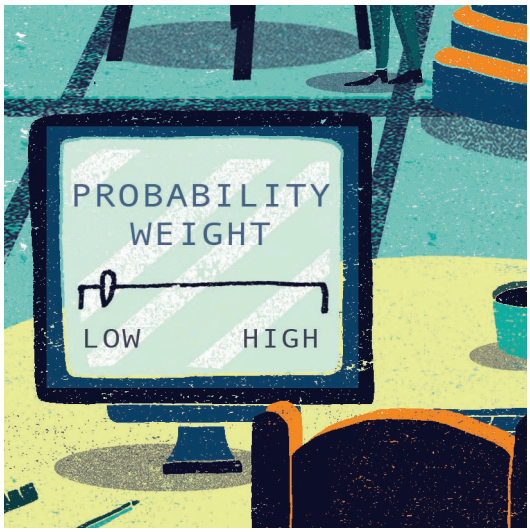
involves challenges similar to those financial institutions often face, among them the perennial issue of data quality. Some fundamental data used in cyber risk models, such as frequency of attacks, can be difficult to acquire when the majority of cyber incidents go unreported.[21] Moreover, the extensive data sets needed to model the probability of cyberattacks are still being developed. One outcome of the Partnering for Cyber Resilience initiative is for participants to collaborate on devising an approach to "near-real-time information sharing [that] can address data availability challenges and supply enough data to build statistical models."[22] This undertaking, along with individual companies' efforts to better understand and characterize their internal data—for example, quantifying the relationship between enterprise assets and the company's revenue and profit picture—are vital to the efficacy of cyber VaR and other cyber risk quantification models.

Other challenges, more organizational in nature, include persistence of operational silos, lack of communication, and inadequate governance. Among these, inadequate governance, along with overdependence on the risk models, has perhaps the greatest potential to foster a false sense of security.

KEY TAKEAWAY Growing cyber risks are compelling organizations to consider the use of risk models. The valuable information that risk models such as VaR can provide should be weighted along with other inputs. To carefully structure and manage cyber risk activities, organizations must prevent any one input from having outsized influence.

GOVERNING THE USE OF MODELS IN CYBER RISK MANAGEMENT

AMONG the desirable attributes of a cyber VaR model highlighted by the Partnering for Cyber Resilience initiative is the model's potential to serve as an effective risk measurement tool for executives and decision makers. One key element of fulfilling this role is that the model be viewed through the lens provided by a company's existing enterprise risk management framework, such as the Internal Control—Integrated Framework or the Enterprise Risk Management Integrated Framework developed by the Committee of Sponsoring Organizations of the Treadway Commission.[23] The components of internal control typically include, at a high level:



- The *control environment* overseen by the board of directors
- A *risk assessment* taking into account operations, reporting, and compliance objectives and the potential impact of cyber risk on them
- *Control activities* aimed specifically at managing cyber risks within the organization's risk tolerance
- Management of *information and communications* relating to cyber risk generally and specific cyber risk events
- *Monitoring activities* that evaluate the effectiveness of internal controls that address cyber risks[24]

Viewing cyber VaR through this lens provides the board of directors and senior executives with an established, effective approach to com-

municating business objectives, their definition of critical information systems, and their appetite for associated cyber risks. In turn, that guidance from the board and senior management sets the tone—and establishes expectations—for rigorous cyber risk analysis across the enterprise.

By embedding cyber VaR within the broader enterprise risk management framework, Partnering for Cyber Resilience suggests, a company's cybersecurity program can be reinforced with "continuous and proactive engagement from senior management."[25] In a 2015 speech, Cyril Roux, deputy governor (financial regulation) of the Central Bank of Ireland, expanded on the importance of management engagement when he outlined the bank's expectations of financial firms with respect to cybersecurity. The themes Roux articulated provide helpful guidance for businesses in any industry seeking to strengthen their ability to detect, prevent, and recover from cyber intrusions. Among them:

- **The board should have a good understanding of the main risks.** This will help board members effectively challenge senior management on the security strategy.
- **Perform risk assessments and intrusion tests.** Organizations should perform cybersecurity risk assessments on a regular basis.
- **Prepare for successful attacks.** Organizations build resilience through distributed architecture, multiple lines of defense, and readiness to mitigate impact on customers.
- **Manage vendor risk.** Organizations should perform cybersecurity due diligence on prospective and existing outsourced service providers, and incorporate cybersecurity and data protection provisions into outsourcing agreements.
- **Gather information and follow leading practices.** Organizations should follow and apply industry standards to their cybersecurity risk-management frameworks as appropriate for the scale and nature of their business and participate in industry information-sharing groups.
- **Educate staff.** Organizations should address the "human factor" through regular security awareness training for all staff.
- **Put robust IT policies, procedures, and technical controls in place.** These include incident reporting and response plans, recovery and business continuity plans, patch management, and employee access rights.
- **Consider buying cyber insurance.** Organizations may consider evaluating the possibility of using cyber insurance as a partial risk-mitigation strategy.[26]

The importance of the first theme in the list above cannot be overstated. The board and se-

nior management should challenge one another to critically analyze and weigh all risk inputs. Key elements of board risk oversight include:

- Communication between the board of directors and members of senior management
- Communication among the board of directors, board committees, and board advisors
- Efficient coordination through a straightforward risk management process uncluttered by too many participants
- Expecting the unexpected through activities such as discussion and analysis of possible risk scenarios with the management team[27]

The last of these four items points to an opportunity for boards to actively engage their management teams in reviews of various risk scenarios. This approach can help boards understand whether the management teams are taking effective action in their risk management processes and can identify areas where improvement is needed.

Some boards may assign responsibility for risk management oversight to their audit committees. They may also want to consider forming a stand-alone cyber risk oversight committee that engages regularly and directly with executives across the organization who are tasked with cyber risk management.

Education of boards, and of senior executives, about cyber risks is central to strengthening directors' roles in addressing these threats. Tools such as *The cyber-risk oversight handbook*, published by the National Association of Corporate Directors (NACD),[28] and guidance from sources such as *Managing cyber risk: Are companies safeguarding their assets?*, published by NYSE Governance Services,[29] can be useful in such efforts.

KEY TAKEAWAY Boards and senior management have an increasing responsibility to monitor their organization's cybersecurity posture, provide oversight of cybersecurity strategy execution, and be prepared to respond to investor, analyst, and regulator questions about actions taken around cybersecurity. Cyber VaR and other risk inputs play a valuable role in fulfilling that responsibility.

LEARNING FROM THE PAST TO PREPARE FOR THE FUTURE

BUSINESS leaders increasingly recognize that quantifying cyber risk is essential to understanding its potential consequences and allocating resources to protect digital assets. As we have seen, whether dealing with financial or cyber risks, risk models can play an important role in addressing threats. Models aid in identifying and evaluating data patterns and trends, a key dimension of the quantification process, along with sound governance processes, available risk data, and skilled cybersecurity and analytics specialists.

At the same time, relying too heavily on the models while ignoring or subordinating other considerations, can open the door to disastrous consequences. Instead, it is important to develop well-defined cyber risk models that align with the nature of a given business.[30] Companies can translate the outputs from these risk models into simple-to-understand concepts that can be used to initiate frank risk-reward conversations across various levels of management and the board. The concepts can help increase these stakeholders' understanding of both the dangers and potential opportunities associated with cyber-related risks in the context of business innovation and growth. In conveying these concepts, it is important to avoid creating a false sense of precision about the models, especially given the lack of empirical data available for certain model inputs.

By keeping the role and importance of models in context when applying them to a cyber-threat environment, businesses and regulatory authorities can enhance their risk intelligence and improve their stewardship in the interest of investors and customers.

JR Reagan *is global chief information security officer of Deloitte Touche Tohmatsu Limited.*

Ash Raghavan *is a principal in Deloitte & Touche LLP's Cyber Risk Services practice and global leader of Deloitte's cyber risk center of excellence.*

Adam Thomas *is a principal with Deloitte & Touche LLP in Deloitte's Cyber Risk Services practice, specializing in cyber insurance.*

Endnotes

1. Joe Nocera, "Risk mismanagement," *New York Times Magazine*, January 2, 2009, http://www.nytimes.com/2009/01/04/magazine/04risk-t.html?_r=1.

2. Mike Billings, "The daily startup: Increased spending in cybersecurity drives funding surge," *Wall Street Journal*, February 17, 2016, http://blogs.wsj.com/venturecapital/2016/02/17/the-daily-startup-increased-spending-in-cybersecurity-drives-funding-surge/.

3. Research shows that risk tolerance changes with context. For example, stock market investors are more likely to be tolerant of larger risks when the market is high than when it is low. This may seem like common sense, but it helps to frame why some executives do not heed the risk models that they themselves implement. For more information, see Yao et al., "Changes in financial risk tolerance, 1983–2001," *Financial Services Review* 13, no. 4 (2004): pp. 249–266.

4. Investopedia, "Value at risk—VaR," http://www.investopedia.com/terms/v/var.asp#ixzz436g0659c, accessed May 6, 2016.

5. Nocera, "Risk mismanagement."

6. "Black swan" is a metaphor coined by risk analyst Nassim Nicholas Taleb to describe highly improbable events with outsized impact, in his book, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*, Incerto series, book one (New York: Random House Trade Paperbacks, 2005, 2nd edition).

7. Sam Fleming, "Market watchdog warns on danger of cyber attack," *Financial Times*, August 24, 2014, https://next.ft.com/content/82519604-2b8f-11e4-a03c-00144feabdc0.

8. Depository Trust & Clearing Corporation, "Over 60 percent of risk managers at financial services firms believe probability of a high-impact event has increased, according to new DTCC survey," December 1, 2015, http://www.dtcc.com/news/2015/december/01/financial-services-firms-believe-probability-of-a-high-impact-event-has-increased.

9. David Sanger, "Utilities cautioned about potential for a cyberattack after Ukraine's," *New York Times*, February 29, 2016, http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyber-attack-after-ukraines.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0.

10. US Computer Emergency Readiness Team, "Alert (TA16-091A) ransomware and recent variants," March 31, 2016, https://www.us-cert.gov/ncas/alerts/TA16-091A.

11. Barbara Vergetis Lundin, "Oblivious in energy: Cyber attacks more successful than ever," SmartGridNews.com, April 8, 2016, http://www.smartgridnews.com/story/oblivious-energy-cyber-attacks-more-successful-ever/2016-04-08.

12. US Office of Personnel Management, "Cybersecurity Resource Center: Cybersecurity incidents," https://www.opm.gov/cybersecurity/cybersecurity-incidents/, accessed April 8, 2016.

13. World Economic Forum, *Partnering for cyber resilience towards the quantification of cyber threats*, January 2015, http://www.weforum.org/reports/partnering-cyber-resilience-towards-quantification-cyber-threats.

14. Ibid.

15. Ibid, p. 12.

16. Ibid.

17. Ibid.

18. Amy Poster and Elizabeth Southworth, "Lessons not learned: The role of operational risk in rogue trading," *Risk Professional*, June 2012.

19. Jody Westby, "How boards and senior executives are managing cyber risks," Carnegie Mellon University CyLab, May 16, 2012, http://www.hsgac.senate.gov/download/carnegie-mellon-cylab-cybersecurity-report.

20. José Manuel González-Páramo, "Rethinking risk management: From lessons learned to taking action," Risk and Return South Africa Conference, March 4, 2011, https://www.ecb.europa.eu/press/key/date/2011/html/sp110304_1.en.html.

21. Center for Strategic and International Studies and McAfee, *Net losses: Estimating the global cost of cybercrime*, June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

22. World Economic Forum, *Partnering for cyber resilience*, p. 15.

23. COSO, "Guidance on internal control," http://www.coso.org/ic.htm, accessed May 6, 2016.

24. Mary Galligan and Kelly Rau, *COSO in the cyber age*, Committee of Sponsoring Organizations of the Treadway Commission and Deloitte, January 2015, p. 3, http://www.coso.org/documents/coso%20in%20the%20cyber%20age_full_r11.pdf.

25. World Economic Forum, *Partnering for cyber resilience*, p. 15.

26. Cyril Roux, "Cybersecurity and cyber risk," address to Society of Actuaries in Ireland Risk Management Conference, Dublin, September 30, 2015, http://www.bis.org/review/r151002d.htm.

27. David A. Katz, *Boards play a leading role in risk management oversight*, Harvard Law School Forum on Corporate Governance and Financial Regulation, October 8, 2009, https://corpgov.law.harvard.edu/2009/10/08/boards-play-a-leading-role-in-risk-management-oversight/.

28. National Association of Corporate Directors, *Cyber-risk oversight handbook*, June 10, 2014, https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688.

29. NYSE Governance Services, *Managing cyber risk: Are companies safeguarding their assets?*, https://www.nyse.com/publicdocs/nyse/listing/NYSE_Governance_Services_Managing_Cyber_Risk.pdf, accessed May 6, 2016.

30. One example of a tailored approach to quantifying cyber risk is provided in "The hidden costs of an IP breach" elsewhere in this issue of *Deloitte Review*, in which the authors demonstrate a scenario-based method for anticipating the impact of a particular type of cyberattack an organization could experience. See Emily Mossburg, J. Donald Fancher, and John Gelinne, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," *Deloitte Review* 19, July 2016, http://dupress.com/articles/loss-of-intellectual-property-ip-breach.

The hidden costs of an IP breach

Cyber theft and the loss of intellectual property

By Emily Mossburg, J. Donald Fancher, and John Gelinne

IT'S A BUSINESS LEADER'S NIGHTMARE—the stomach-churning realization that a corporate network breach has occurred, and that valuable intellectual assets are now in unknown hands. For a US government lab, it could be foreign agents stealing blueprints for a new weapon system; at a biopharmaceutical firm, staff scientists might take confidential data on a potential cancer cure; or at a game developer, hackers could filch the latest first-person shooter game, pre-release. And most terrifying: Because the information exists in the form of data rather than, say, manila folders in file cabinets, a breach might remain undiscovered for weeks or months.

Compared with more familiar cybercrimes such as the theft of credit card, consumer health, and other personally identifiable information (PII)—which regulations generally require be publicly reported—IP cyber theft has largely remained in the shadows.

These kinds of scenarios keep executives up at night for good reason: Intellectual property (IP) is the heart of the 21st-century company, an essential motor driving innovation, competitiveness, and the growth of businesses and the economy as a whole. Intellectual property can constitute more than 80 percent of a single company's value today.[1] It's no surprise, then, that thieves—armed with means, motive, and opportunity—are in hot pursuit.

Though IP theft is hardly new, and some IP may still be attainable only through physical means, the digital world has made theft easier.[2] According to US Intellectual Property Enforcement Coordinator Danny Marti, "Advancements in technology, increased mobility, rapid globalization, and the anonymous nature of the Internet create growing challenges in protecting trade secrets."[3] (See the sidebar "US administration's commitment to trade secret protection.")

Yet, compared with more familiar cybercrimes such as the theft of credit card, consumer health, and other personally identifiable information (PII)—which regulations generally require be publicly reported—IP cyber theft has largely remained in the shadows. Most cases don't receive widespread attention, perhaps because the impact to the public is less direct—and because, considering the potential brand and reputational damage, companies have little incentive to report or publicize such incidents. Plus, compared with PII breaches, IP theft has ramifications that are harder to grasp: fewer up-front, direct costs but potential impacts that might metastasize over months and years. Theft of PII might quickly cost customers, credit ratings, and brand reputation; losing IP could mean forfeiture of first-to-market advantage, loss of profitability, or—in the worst case—losing entire lines of business to competitors or counterfeiters.

Leaders may, understandably, struggle to accurately measure such indirect hypothetical impacts; as a result, behind closed doors, they rarely give IP cyber theft the attention it deserves.[4] Without considering the broad ramifications of a cyberattack involving enterprise IP, companies often neglect to appropriately prioritize IP protection and incident readiness.

The good news for executives is that there is an approach to value the spectrum of losses from IP cyber theft, based on generally accepted valuation and financial modeling principles, so that they can position IP within a broader

US ADMINISTRATION'S COMMITMENT TO TRADE SECRET PROTECTION

The President[5] continues to remain vigilant in addressing threats—including corporate and state-sponsored trade secret misappropriation—that jeopardize the United States' status as the world's leader for innovation and creativity. Advancements in technology, increased mobility, rapid globalization, and the anonymous nature of the Internet create growing challenges in protecting trade secrets. Through a coordinated, multiagency, and multifaceted strategy, this Administration continues to engage foreign governments to strengthen international enforcement efforts, promote private and public sector initiatives to develop industry-led best practices to protect trade secrets, and raise public awareness to inform stakeholders and the general public on the detrimental effects of trade secret misappropriation to businesses and the US economy.

As a part of this strategy, businesses also play a significant role in addressing the growing challenges of protecting trade secrets. The first line of defense against trade secret theft is often the existence of a robust and well-implemented cybersecurity and data management/protection strategy, along with contingency planning in the event of the occurrence of a material event. The Administration encourages companies to consider and share with each other practices that can mitigate the risk of trade secret theft, including approaches to protecting trade secrets that keep pace with technology.[6]

—Danny Marti, US Intellectual Property Enforcement Coordinator, Executive Office of the President

enterprise cyber risk program. With better information about the risks surrounding IP, its potential loss, and the impact this loss could have on the company, executives can understand the full ramifications of IP theft, enabling better alignment of their cyber risk program with the company's IP management and strategic priorities.

THE SHAPE OF MODERN IP THEFT

HISTORICALLY, IP theft primarily took the form of disgruntled or opportunistic employees absconding with documents, computer disks, or prototypes. A wrongdoer had either direct knowledge of, or was able to gain, physical access to perpetrate the crime and extract the trade secrets, in whatever form. The small number of people with physical access limited the pool of suspects, often making such theft a risky proposition.

By contrast, in a digital world, IP thieves can operate from anywhere in relative anonymity, making the pool of possible suspects both wide and deep. Perpetrators can include current and former employees, competitors, criminal and recreational hackers, and foreign-nation state actors. IP theft can be a primary motive—or an opportunistic exploit: When corporate data can more easily be stolen in bulk, the odds increase that nuggets of IP can be found within broad swathes of data.[7]

When being first to market can dictate market winners, stealing IP—or purchasing

stolen IP—can be much faster and cheaper than investing to innovate from scratch. In some fields, research and development (R&D) costs are escalating, while market opportunities are shrinking. With, for instance, a finite number of viable oil fields and high barriers to creating a new patentable drug to treat a particular condition, theft of a competitor's trade secret might promise a more certain path to quick profit.

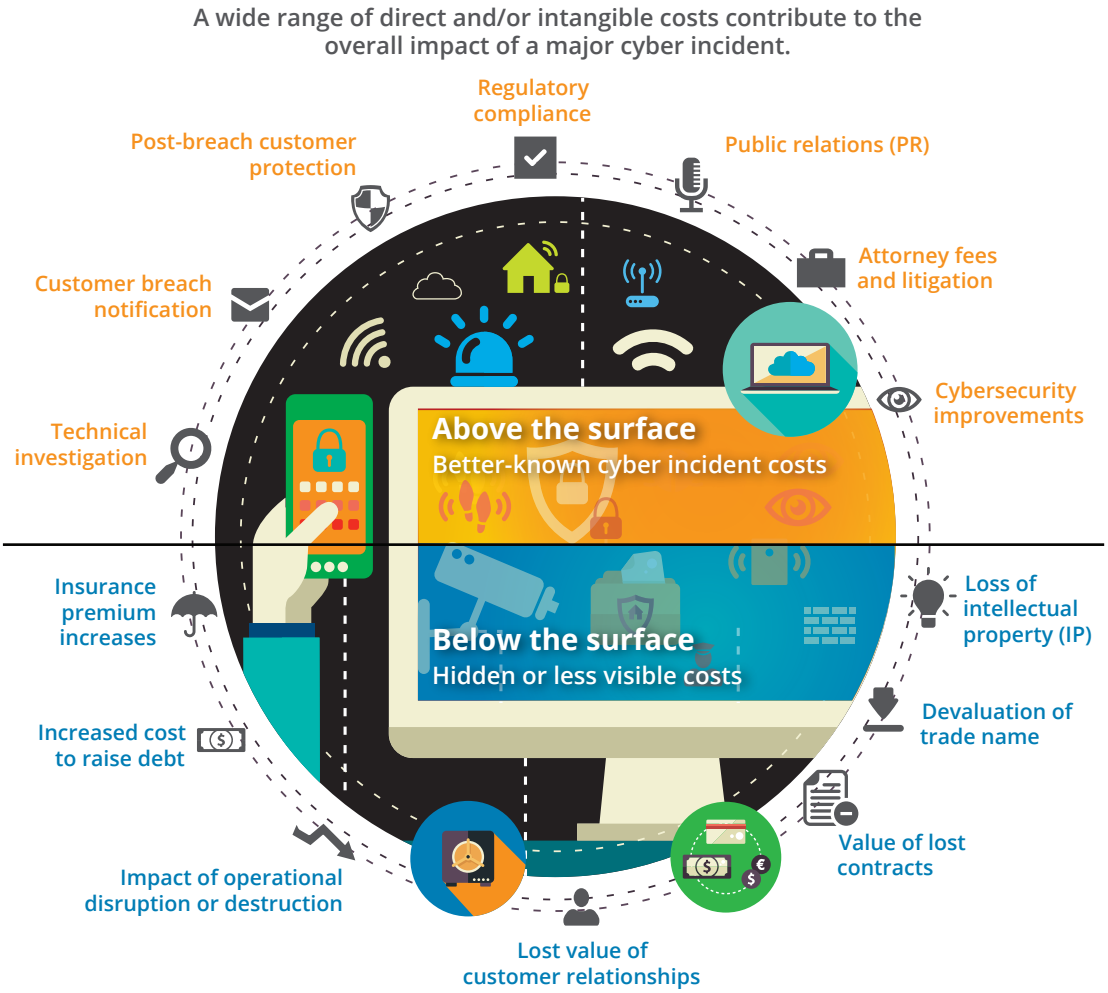
What assets are most at risk? Naturally, thieves are primarily after corporate secrets, rather than IP already in the public domain, such as patents and trademarks. Most valuable to perpetrators are trade secrets and proprietary business information that can be monetized quickly. Trade secrets can include drug trial data, a paint formula, a manufacturing process, or a unique design; proprietary business information might include a geological survey of shale oil deposits, merger plans, or information about business negotiations and strategies. Copyrighted data, such as software code for data analytics, is also now a popular target. With such a broad scope of information of value in different illicit marketplaces, IP theft is an issue across nearly every industry and sector.

VALUING THE SPECTRUM OF IP CYBER THEFT LOSSES

COMPLIANCE and regulatory disclosure requirements generally shape corporate attention to the impact of cyberattacks. In light of well-publicized incidents at leading retail chains, health care companies, banks, and government agencies, those requirements largely center on the theft of PII, payment data, and personal health information. Most American states require organizations to disclose such attacks to customers and employees whose information may have been stolen,[8] and federal securities regulations require corporate disclosure of significant PII-related cyber events with potential material impact.[9] As a consequence, corporate discussions about the impact of cyberattacks tend to focus on costs common to these types of attacks, including those for customer notification, credit monitoring, legal judgments, and regulatory penalties. It helps that there's plenty of precedent, based on those high-profile data breaches, to help executives calculate their companies' exposure in case of a PII leak.

In contrast, when it comes to speculating about the cost of potential IP breaches, many of those costs are "hidden" or indirect and therefore difficult to identify and quantify (figure 1). They include not only well-understood cyber incident costs—such as expenses associated with regulatory compliance, public relations, attorneys' fees, and cybersecurity improvements—but also less visible and often intangible costs that stretch out over months or even years, including devaluation of trade name, revoked contracts, and lost future opportunities. As challenging as it may be for executives to assess these longer-term and indirect costs, identifying and quantifying the full gamut of

Figure 1. Fourteen cyberattack impact factors



Graphic: Deloitte University Press | dupress.deloitte.com

potential IP losses is essential to a company's ability to prioritize its cyber defense efforts.[10]

In considering the applicability of financial risk models to cyber risk, "Quantifying cyber risk," elsewhere in this issue of *Deloitte Review*, asserts that while standard models can be useful, it is important to develop well-defined cyber risk models that align with the nature of a given business.[11] The approach illustrated here considers the specific circumstances of an organization at a particular point in time.

To create the accurate estimates of cyber risk needed to make informed decisions, executives must understand exactly how the full range of impacts might play out over time. To do this, a company should consider a time frame

encompassing the potential long tail following a breach, which can be roughly broken into three phases:

- **Incident triage.** In the days or weeks after the discovery of the attack, the company scrambles teams to analyze what happened, plug any evident gaps, implement emergency business continuity measures, and respond to legal and public relations needs.

- **Impact management.** In subsequent weeks and months, the company takes reactive steps to reduce and address the direct consequences of the incident, including the stand-up of activities to repair relationships, IT infrastructure, or growing legal challenges.

- **Business recovery.** In the following months and years, the company proactively repairs damage to the business, aims to counter measures by competitors looking to profit from stolen information, and shores up its cyber defenses with a focus on longer-term measures.

To model the costs within each phase, organizations can apply a multidisciplinary approach, using knowledge of their business alongside a likely cyberattack scenario to understand what actions may be required. They can then apply accepted valuation techniques to calculate the breach's true cost. Mapping these costs across the three phases can then provide business leaders with a more accurate depiction of a company's cyber risks throughout the response life cycle.

SCENARIO: THE WIDE REACH OF A BREACH

To illustrate the valuation process described above, consider the following scenario involving a fictitious US$40 billion IT company. The company, Thing to Thing, develops networking products supporting the management of Internet of Things (IoT) technology.

The Silicon Valley-based company, with 60,000 employees and a 12.2 percent operating margin, has made a significant investment in R&D, production, and marketing to support the development and release of a core IoT network product. Six months before the product launch, a federal agency informs Thing to Thing of a cyber breach at one of its facilities hosting the new innovation. The initial investigation discovers that foreign nation-state cyber thieves have purloined IP relevant to 15 out of 30 network device product lines, projected to contribute one-quarter of the company's total revenues over the next five years. While the hacker's motives are unclear, an analysis concludes that the information could allow the hacker to unearth and exploit previously undiscovered design flaws or, worse, implant malicious code into Thing to Thing's new products. With even more serious implications, 30 days after the breach alert, a prominent

A scenario-based methodology—positing specific breaches of varying scope and severity, and modeling their impact—permits a realistic and revealing exploration of the IP life cycle to more deeply identify potential risks in the movement and storage of sensitive company information, whether they be external, internal, malicious, or accidental.

Silicon Valley blogger reports evidence that the foreign nation-state is reverse-engineering the networking product, suggesting that it could beat Thing to Thing to market and undercut the firm on price.

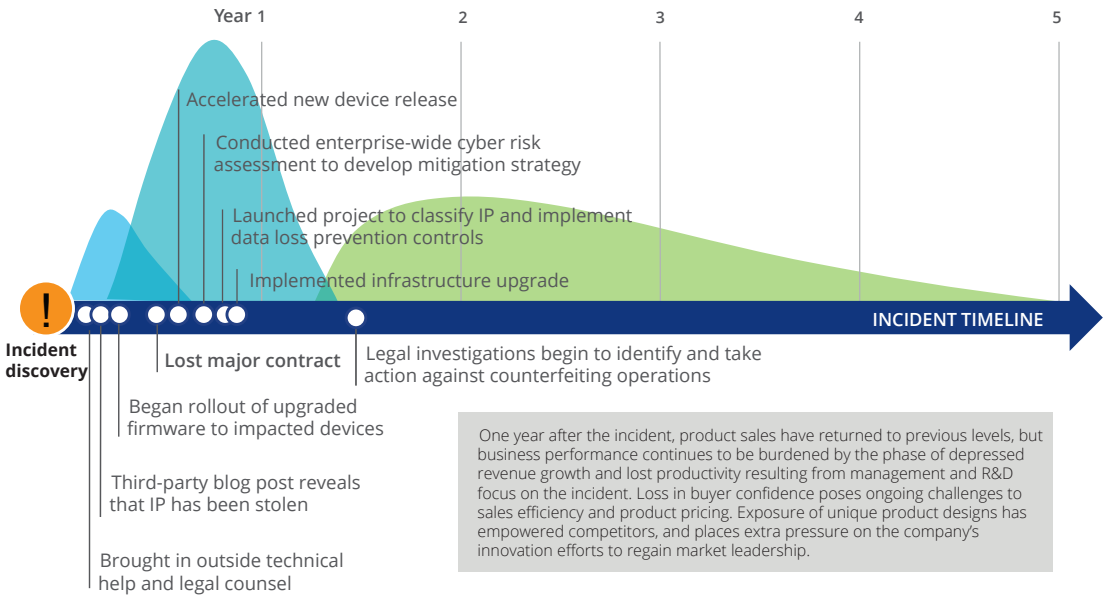
During the initial triage phase, Thing to Thing hires big guns from a top PR firm to reach out to stakeholders and create a face-saving public image campaign. In addition, the company retains attorneys and a forensics firm to investigate the event, and a cybersecurity firm to help triage and remediate the breach.

During the impact management phase, the company is forced to suspend planned sales and shipments of its new products while it develops and rolls out upgraded firmware to affected devices. Although R&D staff are already overextended, Thing to Thing decides to accelerate the new device release by two months rather than be scooped by the cyber thieves—a decision that forces the company to take on additional R&D talent. But loss of confidence in Thing to Thing's ability to protect its own network environment as well as the security of its products intensifies: The government cancels a key contract, projected to contribute 5 percent of revenues, and the company suffers an additional 5 percent drop in revenue as current customers and clients step back.

Longer term, during the business recovery phase, the company conducts an enterprise-wide assessment to develop a stronger cyber risk management strategy and implementation plan. This spawns various initiatives, including an IP inventory, classification, and protection program and enterprise security infrastructure upgrade projects—all of which drive additional costs. Additionally, investigation and litigation costs associated with the breach extend over years, as do PR costs to rebuild consumer and stakeholder trust. Product sales finally return to normal after a year, but business disruption across multiple departments, caused by the redirection of company resources to deal with the breach, drags down operating efficiency.

The cyber incident response timeline in figure 2 describes how the events and impacts of this breach scenario might unfold over time. Of the 14 impact factors that typically comprise the total impact of a cyberattack,[12] some—such

Figure 2. Thing to Thing's cyber incident response timeline



Note: Impact curves illustrate the relative magnitude of costs as they are incurred across the three phases of the response process.

Graphic: Deloitte University Press | dupress.deloitte.com

as breach notification costs or post-breach monitoring offerings—do not apply in Thing to Thing's case, as they might in a PII data breach. The company does face other direct costs associated with legal counsel, PR, investigation, and cybersecurity improvements, which are relatively easy to identify and, to some extent, quantify.

The IP theft's more indirect and deferred costs are harder to identify and to calculate, including the loss of the value of the stolen IP itself, operational disruption, lost contracts, devaluation of trade name, and higher insurance premiums (table 1). In total, over time, Thing to Thing analysts calculate that this one IP cyber theft incident costs the company over US$3.2 billion.

We take two of Thing to Thing's key losses from the IP theft—the networking product's integrity and the five-year government contract—to illustrate the valuation methodologies for less tangible costs. Valuation of both the impact of the stolen IP and the lost contract employs the following generally accepted principles:

- **The with-and-without method.** This approach estimates the value of an asset after an attack, compared with its value in the absence of the theft. The difference is the value of the impact attributed to the incident.

Table 1. What does the attack cost Thing to Thing?

Cost factors	Cost (US$ million)	% Total cost
Technical investigation	1	0.03%
Customer breach notification	Not applicable	0.00%
Post-breach customer protection	Not applicable	0.00%
Regulatory compliance	Not applicable	0.00%
Public relations	1	0.03%
Attorney fees and litigation	11	0.35%
Cybersecurity improvements	13	0.40%
Insurance premium increases	1	0.03%
Increased cost to raise debt	Not applicable	0.00%
Operational disruption	1,200	36.83%
Lost value of customer relationships	Not applicable	0.00%
Value of lost contract revenue	1,600	49.11%
Devaluation of trade name	280	8.59%
Loss of intellectual property	151	4.63%
Total	US$3,258	100.00%

- **Present value of future benefits (and costs).** To calculate an asset's projected benefitswhile accounting for the time value of money, the cost is associated with the specific point in time at which the attack is discovered.

- **Industry benchmark assumptions.** Typical industry benchmarks are used to arrive at the value or financial impact associated with various assets. Examples include royalty rates for the licensing of technology or trade name.

In addition to utilizing these principles to calculate the lost IP's value, the company assumes the IP to have a useful life of five years. We know from the facts set out in Thing to Thing's scenario that the company attributes 25 percent of its total revenue to product lines impacted by the stolen IP. The calculations of financial impact also assume a 2.5 percent royalty rate for potential licensing scenarios associated with the IP, which is based on comparable license agreements for related technologies and the profit margins of public technology hardware companies. This royalty rate is used to ultimately assess value. Finally, based on the risks associated with this type of IP, a discount rate of 12 percent is used to perform the discounting necessary as described above. Applying these financial modeling techniques and the underlying assumptions, analysts conclude that the loss of this IP costs the company roughly US$150 million.

To calculate the value of the government contract, again we consider the facts stated in Thing to Thing's scenario that the contract, covering five years, contributes 5 percent of the

company's total annual revenue. The net cash flows generated by the company over a five-year period with the contract in place were discounted using a 12 percent discount rate to yield a value of US$15 billion. Loss of the contract results in a 5 percent decline in annual revenues and a 2 percent drop in profit margin (with the decline in revenue, the company functions under a lower operating base since its fixed costs are spread over a lower revenue base), resulting in a loss in value of more than US$1.6 billion.

These two examples are only a portion of the total cost of an IP cyber breach as referenced by the above chart. And while a well-meaning executive may not look beyond the (sizable) value of the lost IP itself, the true impact to the business is much greater. In this case, the US$150 million value of the lost IP represents a small fraction of the US$3.2 billion total.

COMPREHENSIVE IP DEFENSE AND RESPONSE READINESS

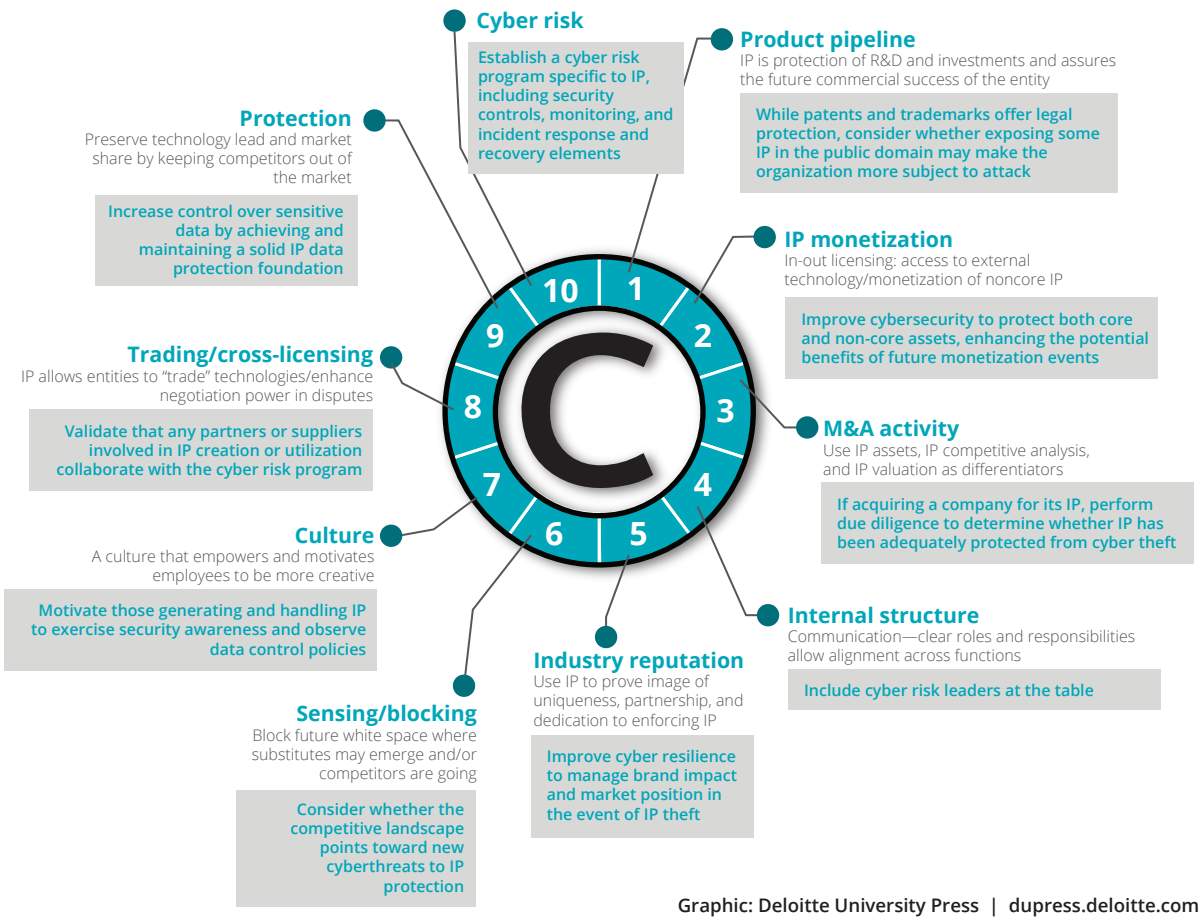
THE goal of the scenario above is not to shock with alarmingly high figures but, rather, to highlight the impacts that matter most in the aftermath of a cyber breach so that executives can understand the full ramifications of IP theft. Once executives realize the importance of protecting digital IP, this scenario can also help guide an examination of their own organization's preparedness. By walking through possible attack scenarios and drafting a truer picture of how the business could be affected, organizational leaders can then create an informed strategy on how they manage cyber risk around the protection of their IP.

A scenario-based methodology—positing specific breaches of varying scope and severity, and modeling their impact—permits a realistic and revealing exploration of the IP life cycle to more deeply identify potential risks in the movement and storage of sensitive company information, whether they be external, internal, malicious, or accidental. Working through a scenario can help quantify the often-hidden costs and wide impact of IP loss. Putting a value on the potential damage and making visible the unseen cost can initiate productive dialogue at the executive and board levels. Equipped with concrete data, executives can then make informed decisions on where best to invest to minimize the costliest impacts. A vague and dreaded threat becomes more defined, and the enemy starts to look like one that can be vanquished with proactive strategies and defenses. Evaluating IP risk across the entire development life cycle turns fear of a potentially devastating cyberattack into confidence: Even if hit by cyber thieves, the organization is positioned to respond and recover.

This increased awareness can then translate to the integration of cyber risk strategies into the company's overall IP management strategy. The *Deloitte Review* article "Wizards and trolls: Accelerating technologies, patent reform, and the new era of IP" outlines nine dimensions that IP strategy should encompass.[13]

Figure 3. Dimensions of an effective IP strategy

The corporate IP management program should be expanded to include a well-defined cyber risk management dimension, and the issues concerning cyber risk should be incorporated as needed within the other nine elements.



Graphic: Deloitte University Press | dupress.deloitte.com

However, as the means and motive for cyber theft increase, leaders should move to include a cyber risk dimension in the company's IP management strategic framework (figure 3). Executive-level governance of the IP program overall must both include explicit oversight of cyber risk management elements and recognize that many of the other IP program elements have associated cyber risk issues.

A more comprehensive cyber risk approach might involve developers, IT, legal, risk management, business, and other leaders to synchronize and align the organization's IP strategy with an effective cyber risk program so that appropriate security controls, monitoring, and response processes are put in place across the IP life cycle. Particularly important is to understand the value of, and safeguard, IP in its early, emerging stages. Relying on IP

protection tactics, such as being "the first to file" or "sensing and blocking" to protect a company's most valuable secrets—while important—fails to recognize that IP has value even before it is "mature." IP in its beginning development stages can be equally valuable to competitors or adversaries long before the decision to file a patent is made. Therefore, the need for speed to protect IP in its digitized form at all stages of its life cycle has increased exponentially—at least commensurate with the speed at which an adversary can gain access to and abscond with a company's most cherished secrets.

Given their importance to growth, market share, and innovation, IP and cyber risk should rightly sit with other strategic initiatives managed at the C-suite level. One important consideration for top executives is to make sure that the cyber risk element of the organization's IP strategy fits into its broader enterprise risk approach and IT/cyber risk framework.[14] For example, the risk assessment methodology and metrics used to assess IP cyber exposures should align with the way other parts of the enterprise measure risks. The entire cyber risk program, including its IP component, should roll up under the organization's enterprise risk management program to give management visibility into IP cyber risks in the context of all risks.

With this contextual awareness of risk, executives can ask hard questions to probe how effectively the company is managing its IP in addition to how well the cyber risk program is

Given their importance to growth, market share, and innovation, IP and cyber risk should rightly sit with other strategic initiatives managed at the C-suite level.

integrated into that process. In practice, these questions might include:

- Where is it possible to reduce the number of people with access to IP?
- Where are the most vulnerable links in the routine handling and protection of IP?
- Is the company's data management/protection strategy sufficient and well understood?
- Are cyber monitoring capabilities aligned and prioritized to detect threats against the company's most strategic IP assets, including fully leveraging private sector–government cyberthreat sharing capabilities?
- If the company's innovation ecosystem extends to partners, suppliers, or third parties, have controls and policies been appropriately extended beyond corporate borders?
- Are well-meaning researchers or developers knowledgeable about the company's

storage, data management, and retention policies so that information is not carelessly left exposed? This last point illustrates that "protection" is not just a technical function but a function of human awareness—people throughout the entire IP life cycle must be made aware of their critical role in guarding valuable corporate secrets.

Finally, while improved security—in the classic sense of policies and technology controls—can improve the odds of preventing a heist, zero-tolerance prevention is impossible. How well an organization responds to a breach can mitigate the toll it takes—a theft need not cost US$5 billion. Incident response is learned through experience, but that doesn't have to mean waiting for a real incident to occur. Simulating cyberattacks provides a practice ground to test the ability of technical and business teams to analyze and restore core mission processes and—more importantly—the ability of the entire organization to act decisively. Practice helps leaders "know what they don't know" and results in better-honed incident response plans for the inevitable "real thing."

CLOSING THE IP EXPOSURE GAP

With the essential contribution of IP to companies' core business and the ever-present danger of IP cyberattacks, managing the risk of IP theft must become an integral part of corporate IP strategy under the purview of the CEO, CFO, general counsel, and, equally important, the CIO and CISO. Corporate IP strategy must include cyber risk elements alongside R&D, patent and copyright, monetization, and other IP plans. Knowing that risks are rising, top executives owe it to investors, employees, customers, and partners to defend IP with the company's best efforts. For corporate leaders and their stakeholders, the goal is the same: protecting and enabling valuable innovations to support the company's future competitiveness and growth.

In doing so, building true resilience requires a firm-wide strategic focus from the top of the organization on the overall business risk that IP cyber theft poses. Knowing exactly what IP a company possesses, where and how that IP is safeguarded, and incorporating IP cyber protection into the overall IP management program should be integral to strategy. When IP is the driver of growth and competitiveness for so many companies, understanding the full impact of its potential loss or misuse is a good start toward managing the risk and moving from simply recognition to action.

Emily Mossburg *is a principal of Deloitte & Touche LLP and leads the Cyber Risk Services portfolio of Resilient offerings.*

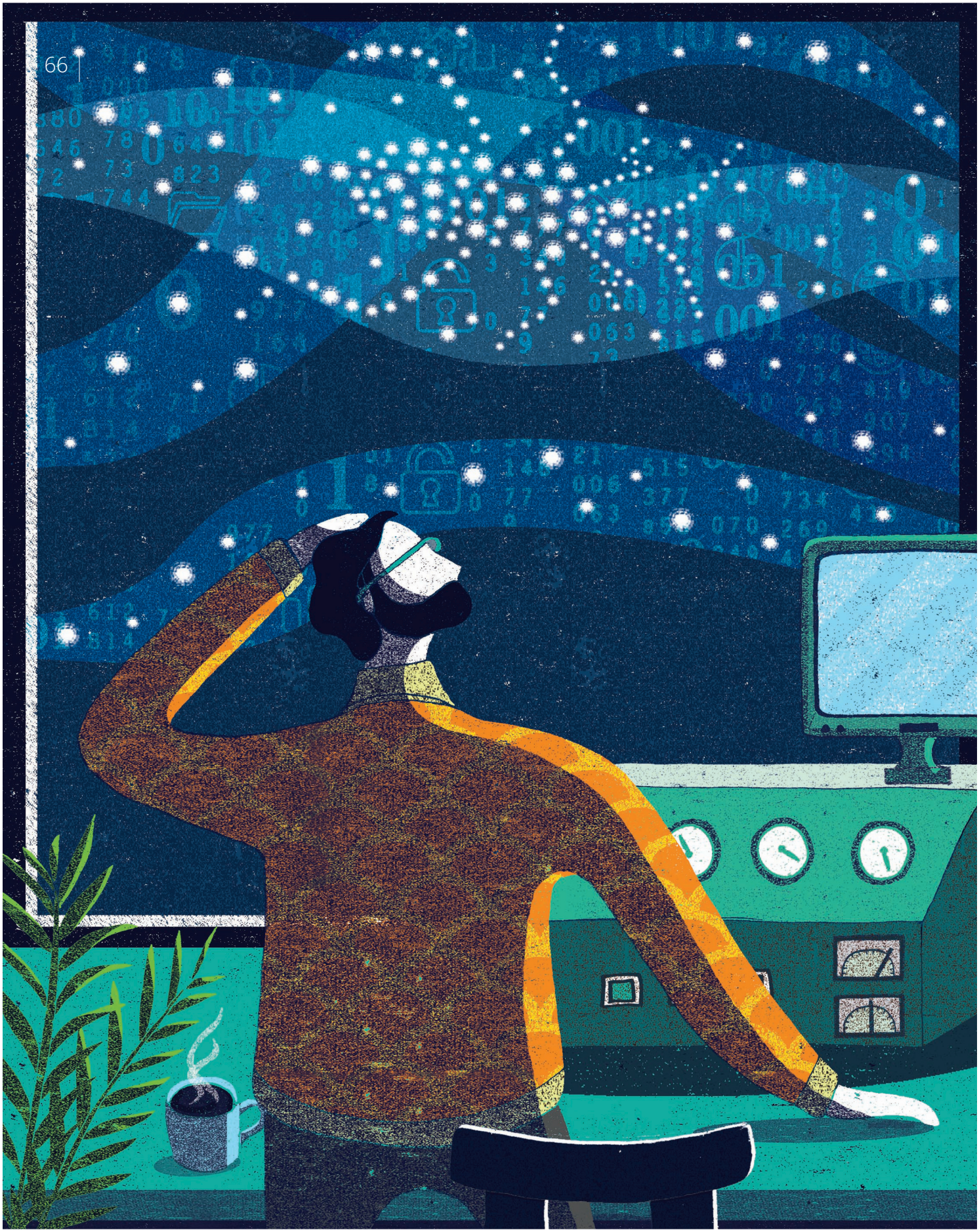
J. Donald Fancher *is a principal and global leader of Deloitte Financial Advisory Services LLP's Forensic practice.*

John Gelinne *is a director in Cyber Risk Services for Deloitte & Touche LLP.*

The authors would like to thank ***Sarah Robinson*** *of Deloitte & Touche LLP for her contributions to this article.*

Endnotes

1. Ocean Tomo, "2015 annual study of intangible asset market value," March 5, 2015, www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/.
2. National Research Council, *The digital dilemma: Intellectual property in the information age*, 2000, www.nap.edu/read/9601/.
3. Danny Marti (Intellectual Property Enforcement Coordinator, Executive Office of the President), statement in email communication with the authors, April 2016.
4. Fred H. Cate et al., "Dos and don'ts of data breach and information security policy," Centre for Information Policy Leadership at Hunton & Williams, March 2009, www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1234&context=facpub.
5. Referring to President Barack Obama.
6. Marti statement, April 2016.
7. In 1971, RAND Corp. analyst Daniel Ellsberg leaked the Pentagon Papers, at the time the largest whistleblower leak in history; over a course of months, Ellsberg had painstakingly photocopied 7,000 pages of secret documents. In contrast, recent leaks based on digital information—Edward Snowden's revelations, the so-called Panama Papers, multiple WikiLeaks data dumps—have involved *terabytes* of private and classified data. Thefts of this scale were impossible before flash drives and the Internet. A target, whenever a leak comes to light, can no longer assume that the leak's scale—and its eventual impact—is limited. See Andy Greenberg, "How reporters pulled off the Panama Papers, the biggest leak in whistleblower history," *Wired*, April 4, 2016, www.wired.com/2016/04/reporters-pulled-off-panama-papers-biggest-leak-whistleblower-history/.
8. A full list of state data breach disclosure laws can be found at the National Conference of State Legislatures site, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, accessed April 18, 2016.
9. No single federal rule or statute governs the loss of all forms of PII. Rules include an OMB rule directing all federal agencies to have a notification policy for PII; relevant legislation may include the HITECH Act, the Federal Trade Commission Act, and the VA Information Security Act.
10. Jess Benhabib et al., "Present-bias, quasi-hyperbolic discounting, and fixed costs," *Games and Economic Behavior* 62, no. 2 (2010): pp. 205–23.
11. JR Reagan, Ash Raghavan, and Adam Thomas, "Quantifying risk: What can cyber risk management learn from the financial services industry?," *Deloitte Review* 19, July 2016, http://dupress.com/articles/quantifying-risk-lessons-from-financial-services-industry.
12. Deloitte Development LLC, *Beneath the surface of a cyberattack*, 2016, http://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.
13. John Levis et al., "Wizards and trolls: Accelerating technologies, patent reform, and the new era of IP," *Deloitte Review* 15, July 28, 2014, http://dupress.com/articles/intellectual-property-management-patent-reform/.
14. One such framework is described by the phrase "secure, vigilant, and resilient." See Deloitte, *Changing the game on cyber risk: The imperative to be secure, vigilant, and resilient*, 2014, www2.deloitte.com/us/en/pages/risk/articles/cyber-risk-services-change-game.html.



From security monitoring to cyber risk monitoring

Enabling business-aligned cybersecurity

By Adnan Amjad, Mark Nicholson, Christopher Stevenson, and Andrew Douglas

Why didn't *we* detect it?

That's the all-too-common question when a major cyber incident is discovered—or, too often, announced. Up to 70 percent of data breaches are detected by third parties rather than by organizations' own security operations teams,[1] a clear indication that most current methods of security monitoring are inadequate.

From a business perspective, for all the money companies spend on the latest detection technologies,[2] IT shouldn't miss anything at all, right? Ironically, the reason so much is being missed may be that IT is capturing too much in the first place: The people with "eyes on the glass" are seeing and evaluating tens or hundreds of thousands of alerts daily.[3] Talent shortages of the right skills exacerbate the problem.[4] Worse, the sea of alerts has no bottom. Cisco estimates that Internet traffic will grow at a compound annual growth rate of 23 percent from 2014 to 2019.[5]

All that data and data-sharing—and the maze of connectivity that moves it all—are the heart of the security problem. As environments grow more complex, they create exponentially more gaps and weaknesses for criminals to exploit—and allow more ways to evade detection.[6] Security operations teams are inundated with IT data being pumped in from millions of devices, detection technologies, and other sources. Detecting what's important has become among the biggest of big data problems, and it doesn't help that many organizations still lack access to the *right* data or the alignment with other departments to even know whether the right data are available.

This is not, as some suggest, just a needle-in-the-haystack problem. Yes, threat detection requires better automated intelligence to sift through all that data. But the latest technologies, alone, will not solve the problem. *IT security monitoring needs to become cyber risk monitoring*. Beyond simply watching for malicious activity, companies need a function that can proactively identify those activities most detrimental to the business and support mitigation decisions.

Naturally, what this might look like will differ from one organization to another, but a new approach should incorporate two basic elements:

- **Business context.** Ironically, making sense of all the IT data requires yet more data, from a wide range of business sources. But more important than mere data collection—and infinitely more challenging—is *linking* it together to put the stream of IT data in context.

- **Business risk guidance.** Technical teams must be equipped with a clear picture of how cyberthreats could most impact the business. This requires engagement across business functions and technical teams so monitoring can be shaped to identify what matters.

A truly risk-focused monitoring function enables organizations to advance their business strategies more freely—and more safely. But making this transition is not an effort that can be delegated to technical leaders and their teams. It requires guidance, collaboration, and ongoing governance at the executive level.

MONITORING FAILURE

EVEN many forward-thinking companies take a technically driven approach to security monitoring. To illustrate some of the pitfalls of that approach, let's walk through what happens to DriveNice, a fictitious car rental company,[7] when struck with a targeted malware attack. Though obviously simplified, this hypothetical scenario (see next page) reflects common, real-world challenges that organizations face.

DriveNice's security operations team, even with relatively low headcount, had no reason to feel especially vulnerable. The chief informa-

WHAT HAPPENED TO DRIVENICE IS NOT SO NICE

DriveNice is a global car rental brand comprising regional companies on five continents, with both corporate and franchise operator locations operating under a central brand. Each region and location has a similar technology platform, with some variations, and uses a mix of regional and centralized IT and security operations. Cloud-based systems are used extensively through a number of service providers, enabling DriveNice to rapidly scale its systems as it expands geographically.

A front-desk employee at a franchised location in Germany opens an email from a DriveNice address and clicks on the harmless-seeming attachment. But the message was sent from a former contractor's account that was never disabled, and the attachment is malware that rapidly spreads through the company's systems. After several weeks, a junior analyst in the central monitoring team discovers the malware and classifies it as a low-risk commodity threat, based on alerts automatically generated by the company's intrusion detection systems.

Because IT manages most such events at a regional level, the analyst writes a ticket on the incident and passes it to the regional business units for prospective follow-up. Unfortunately, the analyst lacks direct access to the actual devices that are generating the alerts, so the report goes out with limited information. Because of the low-risk classification, the analyst considers the case closed after he sends the alert to the regional units; in a poor attempt at tuning, he configures the monitoring system to disregard future events of the same type.

Weeks later, 3 million customer payment records show up for sale on a cybercriminal forum. DriveNice learns of the issue when a journalist contacts the press office, seeking comment.

While IT scrambles to understand the nature of the breach and coordinate multiple security teams, the malware itself has already begun its second phase. It has turned out not to be a common, low-risk threat—hackers customized it to target DriveNice, with code written to access the company's NiceRewards loyalty points system and manipulate customer account balances. Since the NiceRewards platform is cloud-based, DriveNice's control and visibility are severely limited; engineers did not have the ability to incorporate security events from the application into the company's security monitoring systems.

When members start complaining that their point balances are inaccurate, the NiceRewards team begins investigating potential business logic problems. Separately, the fraud team has noticed suspicious loyalty-point usage trends: A higher-than-usual number of customers are cashing out loyalty points for gift cards or points in partner rewards programs. The fraud and SpeediReward teams, heavily involved in business analysis and response to the original breach, are unable to give the new concerns their full attention.

Another month goes by before anyone links the three events—the payment breach, the ongoing discrepancies in NiceRewards accounts, and fraudulent cash-outs—as associated with the same malware incident. By this time, customer dissatisfaction is growing louder, costs from the payment breach are mounting, and DriveNice fears that negative press coverage may be having an impact on revenue. To avoid potential losses, rewards-program business partners have suspended integration with DriveNice's program, and franchisees are growing frustrated—shouldn't headquarters have fixed these problems by now?

tion security officer (CISO) believes her team, watching dozens of screens, is doing pretty well at following leading practices, especially after making investments enabling them to centralize and correlate reams of data from a wide range of security tools. They've recently upgraded their security operations center and launched a data loss prevention initiative. They purchase threat intelligence to help understand the landscape of potential malicious activity. Notwithstanding the company's extensive and diverse infrastructure, the team does a pretty good job of patching critical systems. Although the central monitoring team lacks full visibility across the network, the CISO has actively encouraged them to share communications. What's more, they regularly pass their compliance exams.

What went wrong?

It'd be too easy to blame the DriveNice breach solely on any individual error or oversight. The company's fundamental IT-based approach to security monitoring contributed to both the failure and the weeks it took to discern the attack's full scope.

First, DriveNice missed early warning signs when the malware first appeared on the mail server. As frequently happens, the initial download could have evaded detection because threat intelligence feeds did not yet list the source as malicious; the malware was different enough from known threats that security tools could not yet detect it.[8] However, other signs should have been visible. While the front-desk employee could hardly be expected to know it, the phishing email containing the malware link was from the address of a former contractor whose account should have been deactivated months ago. If, in addition to the volumes of IT system data, security operations had utilized current records from the HR department, they could have detected the use of an obsolete account, raising an immediate red flag.

Second, when the security team finally did detect malware, they failed to understand that the attack was both serious and targeted. The analyst's performance was understandably impacted by the number of screens he was assigned to review as well as by the limited information that security technologies generated. In addition, he was hampered by the system's inability to see which regional locations might be seeing the same type of event.

A culture of passing responsibility also contributed to the problem: Where multiple teams are involved, it is easy for problems to be "thrown" but not "caught." DriveNice, like many companies, suffered from a lack of consistent oversight and centralized workflow management. These factors, compounded by human error, led to the system being configured to tune out future similar events—common when junior staffers are left to make decisions without adequate knowledge or training.

And finally, once analysts realized that the malware was significant, they failed to see the

hackers' second—and possibly more fundamental—attack motive. As soon as it emerged that credit card data were involved, responders became focused on a narrow analysis and response process, and task saturation blinded them to other threat activity. IT itself was poorly coordinated, and the central security monitoring team had little visibility into the regional systems that were involved. The use of non-integrated third-party cloud providers left them with sizable blind spots.

Worse, there was a lack of communication at the business level—an obstacle that many executives will find all too familiar. The NiceRewards department knew that customers were complaining about issues with their accounts, and the fraud department had been tracking dubious rewards activity, but no one engaged IT. Yes, correlating this information would have been a manual process, but had the cyber monitoring, fraud, and loyalty program teams been synchronized, a more complete picture of the issues would surely have emerged sooner. In addition, if the CISO had participated in peer or law-enforcement information sharing, she might have known that a competitor was experiencing a similar attack, and been equipped with deeper insight into the operation of the malware.

DriveNice's approach to security monitoring remains IT-centric. As a result, the company faces technical and organizational hurdles that impede its ability to detect the attack quickly and equip responders with actionable information.

MONITORING FOR CYBER RISK MANAGEMENT

In contrast, the monitoring program of the future is focused on cyber risks to the business. This change is an outgrowth of executive—and often board-level—involvement to set the tone and priorities around cyber risk as part of an organization's larger business risk management programs.[9] To achieve this transformation, changes are needed in four key functional areas:

- **Alignment** of the whole organization, horizontally and vertically, around top cyber risks
- **Data** to support business event detection rather than technology event detection
- **Analytics** to transform from an indicator-driven approach to a pattern-detection approach
- **Talent** and talent models to enable evolution from reactive to proactive action models

Before reviewing these four functional areas in greater detail, let's look at how DriveNice, our rental car company, might have fared if, prior to the targeted attack, it had in place a business-focused cyber risk monitoring program (see next page).

DRIVENICE WITH A BUSINESS-FOCUSED CYBER RISK MONITORING PROGRAM

Like any company in its sector, DriveNice is subject to advanced cyberattacks. As in the earlier example, human error results in a company workstation becoming infected with a new variant of targeted malware. The malware is fairly sophisticated and can evade detection long enough to spread fairly quickly to workstations across various regions.

One day, amid the security alerts streaming into DriveNice's monitoring center, one—associated with the central payments system—stands out as a high-priority alert. The system automatically assigns a Level 2 security analyst to investigate; he quickly finds new desktop connections being made. Someone, it appears, has been attempting to access the payments system using some front-desk employees' (valid) credentials. The analyst quickly correlates information about the new connections and determines that they are likely coming from an Internet service provider network in an Eastern European country. Threat information on another console shows that the IP addresses being used are associated with a network that has previously been used for criminal command-and-control network activity. The analyst quickly summarizes known information in the incident ticket, captures the malware code from the end-point analysis tools deployed on workstations, and submits it for detailed forensic analysis.

Although this analysis will take at least 24 hours to complete, he immediately notifies the regional security and IT teams of a potential issue and alerts the payments team to watch for unusual activity. The workflow features in DriveNice's monitoring systems push out critical characteristics (indicators) of the malware to cyber defense teams and tools across the regional IT teams; this automatically prevents DriveNice computers from connecting to the malware's command-and-control service, automates removal of the malware binary where found, and prevents infection of additional systems.

These measures largely purge the malware from the company network and prevent it from accessing payment data, and system administrators are tasked with patching security holes in laptop and desktop systems to prevent similar infections. With the CISO's help, senior analysts compare notes with peers in another organization who experienced a similar attack several weeks prior, to determine whether it is a variant of the same malware. They learn that such malware often executes multiple functions—and that they should prepare for a second-phase attack.

Within 36 hours, the team thoroughly understands the nature of the malware. The CISO immediately convenes a meeting between the regional security teams and representatives from the payments and fraud teams to inform them of what has occurred, answer questions, and alert them to activity they might see if the malware were to spread further.

Because systems in a few regional operations do not yet comply with IT operations standards, a small number of desktops remain infected. These infections allow the malware to launch a second phase of attack, this time against the NiceRewards loyalty program. In the central monitoring center, another high-priority security alert fires, triggered by a behavioral analysis system, indicating that the NiceRewards database server is being accessed from a network in Australia known to be associated with suspicious activity.

Within minutes, the assigned analyst can clearly see a direct database access attack in progress. Using data provided by the loyalty team, he is able to note that a number of customers have reported discrepancies in their rewards point balances—and that these same accounts are being used repeatedly over short intervals to attempt to cash out rewards. Armed with this information and the results of the malware analysis, the monitoring team quickly works with the Australian franchise's IT team to stop the attack (and potentially leverage existing relationships to notify local law enforcement). The loyalty team is able to reverse almost all NiceRewards cash-outs before transactions are completed. The attackers, rapidly detected and shut down, move on to target other, less prepared organizations.

The elements that made a difference

Compared to the earlier scenario, DriveNice has made a number of important changes to its cyber risk monitoring program that have helped the company significantly limit the impact of this attack.

First, technical and nontechnical teams meet regularly to identify emerging dangers most likely to threaten DriveNice's revenue streams, profit margins, and reputation. This has enabled security engineers to configure monitoring technologies to look for specific events and patterns that would indicate possible NiceRewards abuse and fraud. Detection required integrating business data from the loyalty, fraud, and HR departments into the monitoring systems. A small project was undertaken to automate the regular data transfer.

CYBERSECURITY FUSION CENTERS

Companies that are leaders in establishing risk-centered cyber risk operations have modeled their organizations after "fusion centers" that the US government instituted after the attacks of September 11, 2001, to foster cross-agency collaboration on threat assessment and response. In these centers, a multidisciplinary team of professionals from across the organization focuses on adapting to a sophisticated and ever-changing community of adversaries.

This team may have representatives from risk management, internal audit, fraud or anti-money laundering, and legal counsel. On the technical side, it may include leaders from application development, system and networking engineering, cyber risk operations, and leading threat analysts. Business information security officers who report to line of business or regional leaders complete the group. This diverse body not only brings to the table diverse perspectives on business risk and cyber risk, but also enables the "fusing" of a wide range of data, from threat data to business data to IT data, both generated internally and from external sources.

Rather than handing off tasks from one group of experts to another as happens today, the integrated team—especially if members are co-located—can more easily share knowledge about what is happening across the various areas of the business. This enables faster and more effective diagnosis and remediation when incidents occur.

Perhaps most important, the fusion center provides an ongoing working environment that cultivates understanding between business and cyber risk professionals. Participants can continually refresh their understanding of the threat landscape and develop shared focus on the cyber risks that matter. Nontechnical people become better acquainted with technical terms and challenges; technical leaders develop the granular understanding of business processes to know and define more effective monitoring. The fusion-center structure sits at the heart of the organization's ability to proactively refine and adjust detection capabilities as both external threats and the business itself change.

Another outcome of this collaboration was a decision to bring DriveNice's cloud-based assets into the monitoring program, requiring a combination of technical integration efforts and business efforts to negotiate agreements with service providers. When this attack occurred, then, the security team had visibility into application logs that were essential to detecting suspicious activity.

Managers have more clearly defined roles and lines of communication between the fraud and rewards cyber operations, and among the various IT security departments. When the event happened, there was more rapid dialog and action. Although regional teams still exist, event data are centralized, and the teams operate in a far more coordinated fashion, with the central monitoring team having a clear

Growth itself—entering new markets, launching new products, driving efficiencies, or establishing new business models—requires organizations to take risks. Having awareness of how cyberthreats could impede growth and innovation, and visibility to know when the business is actively threatened, are essential to protecting strategic interests. This is the core mission of the new cyber risk monitoring function.

top-down mandate to drive cybersecurity detection.

Business leaders, more attuned to the need to support cyber risk efforts, now routinely consult with cyber risk leaders before making changes to applications and technology infrastructure, and have enforced a program among their own technology teams to regularly provide IT asset updates to the central monitoring operations team.

As executives and business risk leaders gained confidence in the effectiveness of DriveNice's monitoring program, it was easier for IT leaders to gain support for new technology investments. Implementing an end-user behavioral analytics program has provided analysts with better pattern detection capabilities to help identify previously unknown cyberattack tactics.

FOUR CRITICAL TRANSFORMATION AREAS

THE success of DriveNice—in the second hypothetical case, that is—cannot be attributed solely to either enhanced technology or enlightened leadership. It required an evolution that any company can make by undertaking transformations in the four key areas that helped DriveNice thwart the malware and avert the threat.

Alignment around top business risks

Business leaders and their technology teams actively collaborate with cyber risk teams to develop a shared view of the top cyber risks facing the business, and then define key risk indicators: signs that something on the cyber front could be impacting essential business operations and processes. As part of this ongoing process, some organizational restructuring may be needed, including the creation of new functions, departments, or committees. (See sidebar, "Cybersecurity fusion centers.") Equipped with a granular understanding of how business applications and processes work,

engineers can create solutions to monitor the right things, and can also improve their ability to report to executives and business leaders on cyber risk posture.

Leaders can guide this transformation by firmly defining communication channels and roles across the business so that cyber risk analysts know whom to engage, internally or externally, for support in detection, monitoring, analysis, and response. Similarly, the cyber monitoring function would now generate regular reports—in terms meaningful to the whole range of stakeholders—summarizing both cyber risk improvements and current areas of vulnerability to help maintain that alignment.

The right data

As discussed above, monitoring teams today are flooded with data—but not necessarily the right data to detect what matters. By taking a business-driven approach to cyber risk detection, engineers can be more purpose-driven in the data they're capturing, equipping analysts with the data needed to detect cyber *business* events rather than just *technology* events. A technology event—such as an unauthorized person accessing a particular systems—becomes a business event when a cyber analyst can see that the system is part of a key business process, and has some context that ties it to a potential threat.

The key is granting the cyber monitoring team access to timely and relevant data from various parts of the business needed to correlate IT, business, and threat activity. What this looks like will vary from one company to another, but for every organization, it will include some data beyond technical device data. Commonly, this might include lists of current employees, partners, and contractors allowed to access resources. It could also include a wide range of business transaction data, inventory data, and customer service records.

Analytics for better intelligence and automation

The "last mile" effort to detecting meaningful threat activity will always have an important human component, but without the aid of automated intelligence, it is virtually impossible to see threats across a vast and complex environment. Most corporate cybersecurity teams today are equipped with security information, event management, or other tools that can help correlate and filter information requiring human attention. Some organizations can significantly improve by better leveraging what they have.

However, most legacy monitoring tools can detect only yesterday's threats because they rely on matching information to databases of already known threat "signatures." Because threats change daily, many can escape detection. Companies may need to augment existing technologies with newer ones that support a pattern or anomaly-oriented detection approach. Advanced analytics technologies typically can handle significantly greater and more

diverse forms of data, but most important, they provide the flexibility for organizations to create their own threat intelligence. By focusing on understanding what "normal" looks like—such as normal network traffic patterns, volumes of business transactions, and behavior of individual network users—cyber risk operations teams can more quickly and accurately detect anomalies that signal an attack is under way. Given that threat "indicators" change rapidly and attackers frequently modify their approaches, greater emphasis on detecting exceptions to "normal" patterns increases the likelihood of finding the things that warrant serious investigation.

The human element remains critical

CIOs and CISOs worldwide are all too aware of the technical talent shortage in cybersecurity. But companies need not only more skilled people, but also new approaches. Roles need to be established for analysts who routinely think about what could happen rather than primarily reacting to what they see. While patching known system vulnerabilities remains important, cyber risk teams need to find the holes that no one has previously detected—or even looked for.

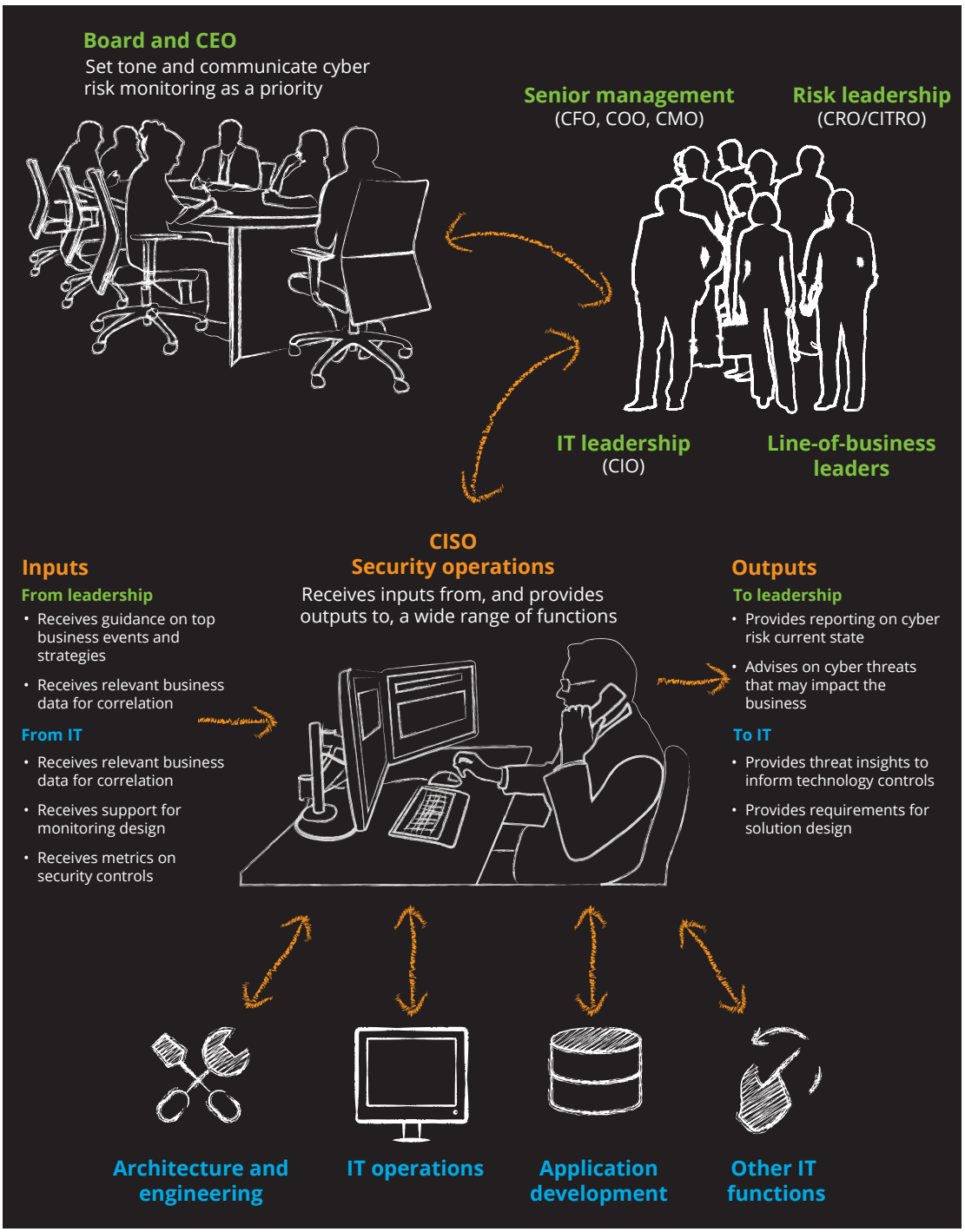
Analysts and cyber engineers at all levels need greater knowledge of core business processes, so they can understand a security incident's business context and design better detection mechanisms; being a "techie" isn't enough. Nor is it enough for the CISO: He or she needs to be capable of fostering the engagement of business units and departments across the organization. (For a discussion of the changing role of the CISO, see "The new CISO: Leading the strategic security organization" elsewhere in this issue.[10]) Conversely, top executives and managers—particularly those involved in driving strategic business innovations—need to know enough about cyber risk to understand when to engage internal or external experts. (See figure 1.)

TOWARD A NEW MONITORING FUNCTION

GROWTH itself—entering new markets, launching new products, driving efficiencies, or establishing new business models—requires organizations to take risks. Having awareness of how cyberthreats could impede growth and innovation, and visibility to know when the business is actively threatened, are essential to protecting strategic interests. This is the core mission of the new cyber risk monitoring function.

It is not a rip-and-replace process or a groundbreaking construction effort—nor should executives feel compelled to abandon the cybersecurity investments they have already made. It is a transformation of existing capabilities that will most likely need to happen over many months, if not years. Fortunately, it can (and should) be an iterative process, building on past efforts.

Figure 1. Broad organizational involvement in a cyber risk monitoring program



Note: CEO = chief executive officer, CFO = chief financial officer, COO = chief operating officer, CMO = chief marketing officer, CRO = chief risk officer, CITRO = chief IT risk officer, CIO = chief information officer.

Source: Deloitte Development 2015.

Graphic: Deloitte University Press | dupress.deloitte.com

Once the organization has matured and encountered the boundaries and limits of what it is working with today, there are many options for advanced technologies that can provide a sound platform for richer analytics-based "cyber hunting" approaches to empower trained analysts to scout for—and even predict—attacks.

Any organization needs *executive-level guidance* on the top areas of cyber risk about which the business should be concerned. Organizations that already have a cyber-aware board and have integrated cyber risk into their overall enterprise risk framework will likely have a clear advantage.

Leadership at the *business unit and department levels* must be willing to pioneer an integration between cyber risk and business risk. On the business side, the organization needs people who are conversant—or want to become conversant—in the high-level concepts pertaining to cyberthreats and cyber monitoring. On the technology side, it's essential to have a CIO or CISO at the helm who can effectively enlist other business leaders in defining the business risk management requirements that need to shape the cyber risk monitoring function. Pockets of leaders in some organizations—unbeknownst within the executive suite—may have taken it upon themselves to drive initiatives in the right direction. Uncovering these and providing additional support might be a way to accelerate pilot efforts that can spur efforts in other parts of the organization.

Finally, the organization needs *engineering talent, operational managers*, and *technologies* sufficient to lead the actual stand-up or extension of monitoring technologies to adapt to the new requirements. The whole effort, however, is not primarily a technical challenge. All too often, there is a silver-bullet mentality—wishful thinking that an emerging technology, solution, or vendor will solve today's security monitoring gaps. More likely, tools and technologies are currently in place that, driven with the right skills and business collaboration, can be better leveraged.

Once the organization has matured and encountered the boundaries and limits of what it is working with today, there are many options for advanced technologies that can provide a sound platform for richer analytics-based "cyber hunting" approaches to empower trained analysts to scout for—and even predict—attacks. Regardless of how sophisticated the tools, deriving meaningful results rests on an underlying principle: Business and cyber risk practitioners must, together, determine what business risks are being addressed, and what

risk indicators are most important before focusing on methodology, data, or technology.

The effort to transform monitoring capabilities is a "living" effort. Ongoing governance is needed to maintain a culture of collaboration to continually improve and support the monitoring program—to ensure that requests from technical teams are given appropriate merit and that technical and business teams maintain a current, shared understanding of the business risk landscape.

At the pace of today's business evolution, it is inevitable that some threats will evade even the strongest security controls, making effective threat detection an essential function to safeguard business growth. For as daunting as the challenge can seem, there is hope. When executives become involved in guiding the alignment of data, analytics, and talent with top business risks, organizations can begin to move from reactive cybersecurity detection to proactive cyber risk management.

Adnan Amjad *is a partner with Deloitte & Touche LLP and leads its Vigilant practice, which includes vulnerability management, security operations design, managed security operations, and cyber threat management analytics.*

Mark Nicholson *is a principal with Deloitte & Touche LLP and a leader of its Vigilant business, primarily serving the financial services industry.*

Andrew Douglas *is a director with Deloitte & Touche LLP and a specialist in the Cyber Risk Services group, with a focus on advanced cyber testing.*

Christopher Stevenson *is a director with Deloitte & Touche LLP with extensive experience building real-time electronic trading, market data, and risk management systems for financial institutions and exchanges.*

The authors would like to especially acknowledge ***Beth Ruck*** *for her leadership and contributions to this article. In addition, we would like to thank* ***Keith Brogan****,* ***Isaac Kohn****, and* ***Jake Skoniecki****.*

Endnotes

1. James Carder, "7 significant insights from the CyberEdge cyberthreat defense report," LogRhythm, February 10, 2016, https://logrhythm.com/blog/7-significant-insights-from-the-cyberedge-cyberthreat-defense-report/.

2. Investment in security information and event monitoring tools alone is estimated to have a compound annual growth rate of 7 percent annually. Gartner, "Forecast analysis: Information security, worldwide, 4Q15 update: IT spending by segment in current dollars, worldwide, 2013–2019 (millions of US dollars)," March 22, 2016.

3. Damballa reports that, daily, "the devices within its average customer's network generate an aggregate average of more than 10,000 events that may potentially be associated with malware behavior." Damballa, *State of Infections Report Q1 2014*, www.damballa.com/damballa-q1-2014-report-shows-average-enterprise-generates-10000-security-events-daily/.

4. In the United States, more than 209,000 jobs in cybersecurity are unfilled, and postings are up by 74 percent. These numbers are expected to grow in the following years. Ariha Setalvad, "Demand to fill cybersecurity jobs booming," Peninsula Press, March 31, 2015, http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.

5. Cisco, *Cisco Visual Networking Index: Forecast and methodology, 2014–2019 white paper,* May 26, 2015, www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.

6. With the growth of underground marketplaces, malware authors have a financial incentive to find new and up-to-date exploits. See Bromium Labs, *Endpoint Exploitation Trends 2015*, 2016, www.bromium.com/sites/default/files/rpt-bromium-threat-report-2015-us-en.pdf.

7. Neither of these scenarios intentionally represents the circumstances or events of any particular company.

8. A December 2013 study found that no anti-virus scanners had 100 percent detection rates, although the highest was 99.9 percent effective. Many anti-virus programs produce false positives, adding to unnecessary noise. See AV-Comparatives, *Whole product dynamic "real-world" protection test*, December 10, 2013, www.av-comparatives.org/wp-content/uploads/2013/12/avc_prot_2013b_en.pdf.

9. For more information on how boards and other leaders can drive cybersecurity changes within their organizations, see Taryn Aguas, Khalid Kark, and Monique François, "The new CISO: Leading the strategic security organization," *Deloitte Review* 19, July 2016, http://dupress.com/articles/ciso-next-generation-strategic-security-organization.

10. Ibid.

TO LEARN MORE, PLEASE CONTACT:

Nick Galletto
Global Cyber Risk Services Leader
+1 416-601-6734
ngalletto@deloitte.ca

James Nunn-Price
Asia Pacific Cyber Risk Services Leader
+61 2-9322-7971
jamesnunnprice@deloitte.com.au

Ed Powers
US Cyber Risk Services Leader
+1 212-436-5599
epowers@deloitte.com

Chris Verdonck
EMEA Cyber Risk Services Leader
+32 2-800-24-20
cverdonck@deloitte.com

Ash Raghavan
Global Cyber Center of Excellence Leader
+1 212-436-2097
araghavan@deloitte.com

Deloitte has been widely recognized as a market leader, including these recent independent analyst reports:

- **Deloitte named a global leader in Security Operations Consulting by ALM Intelligence**
  Source: ALM Intelligence; Security Operations Center Consulting 2015; ALM Intelligence Consulting Research & Advisory estimates © 2016 ALM Media Properties, LLC. Reproduced under license
- **Deloitte ranked #1 globally in Information Security Consulting for 2015 based on revenue by Gartner**
  Source: Gartner, Market Share Analysis: Information Security Consulting, Worldwide, 2015, Jacqueline Heng, Elizabeth Kim, 05 July 2016