Deloitte.
University Press

New perspectives on how cyber risk can power performance

Cyber ●

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.

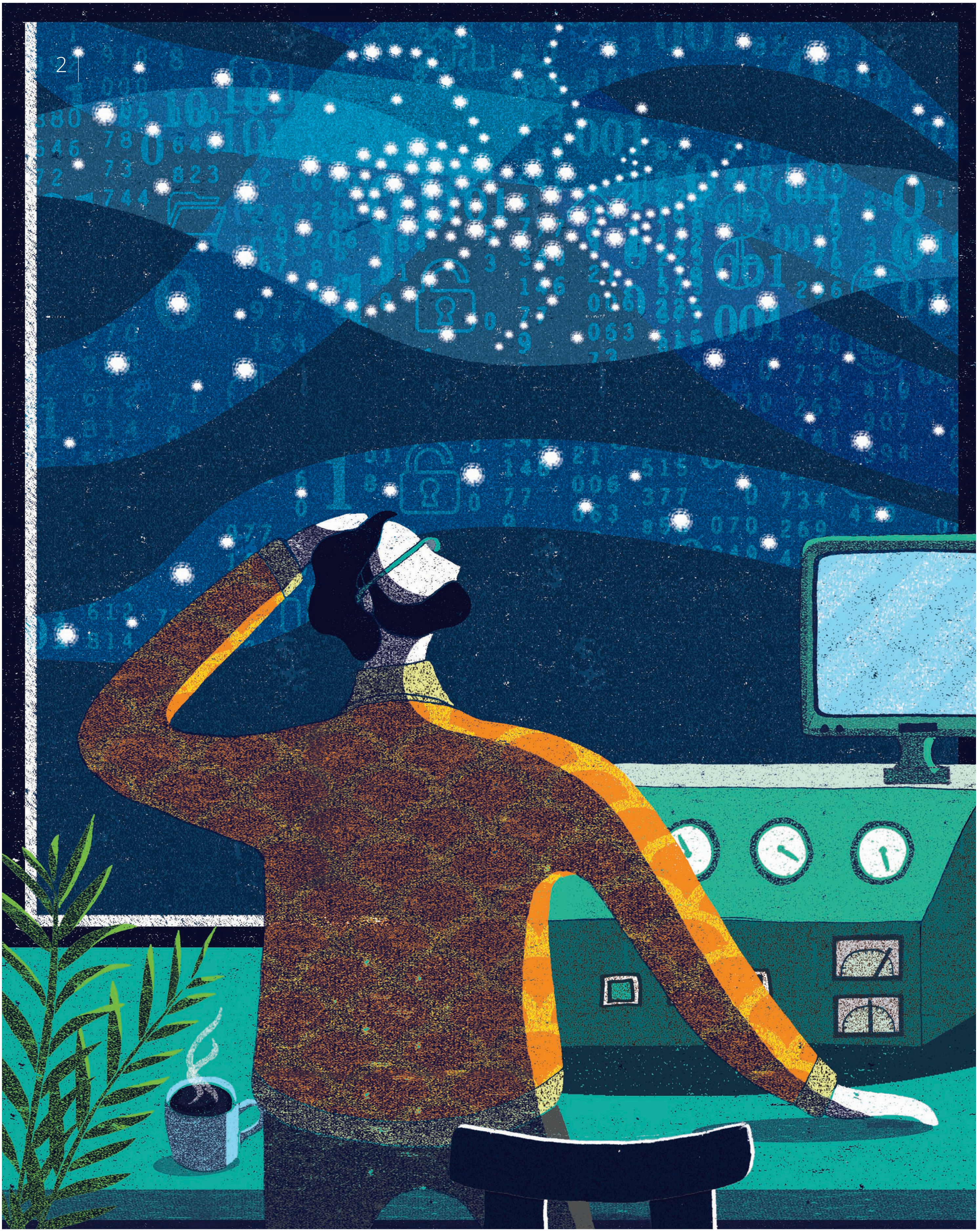
Business leaders understand that doing what needs to be done to create enterprise value often means taking risks. Think about the range of initiatives that today's organizations undertake to pursue innovation, accelerate performance, and enable growth: Using social media tools to attract customers and 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

Sam Balaji
Business Leader
Global Risk Advisory



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.

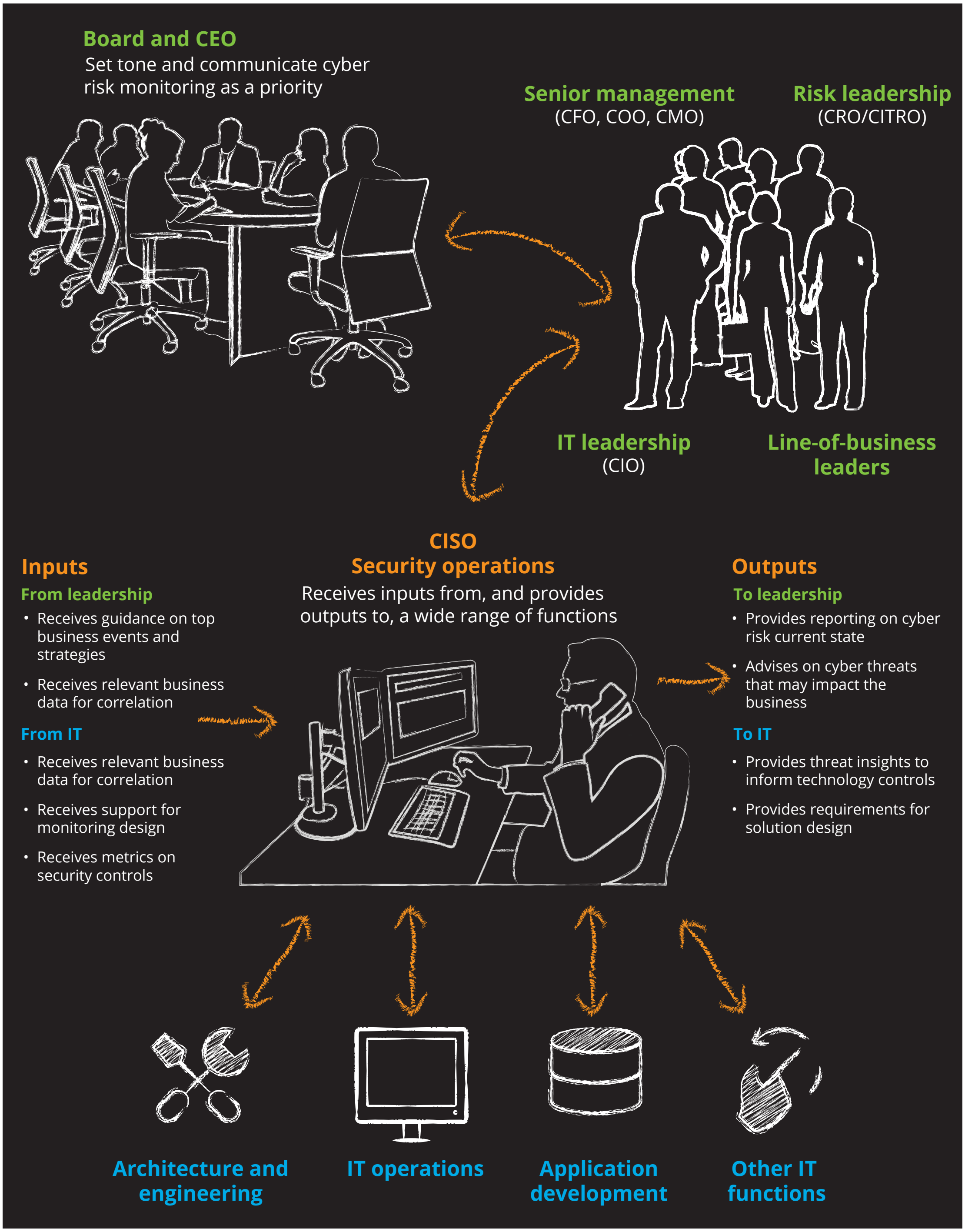
Analysts and cyber engineers at all levels need greater knowledge of core business processes, so they can understand a security incident's business context and design better detection mechanisms; being a "techie" isn't enough. Nor is it enough for the CISO: He or she needs to be capable of fostering 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



Board and CEO

Set tone and communicate cyber risk monitoring as a priority

Senior management
(CFO, COO, CMO)

Risk leadership
(CRO/CITRO)

IT leadership
(CIO)

Line-of-business leaders

CISO
Security operations

Receives inputs from, and provides outputs to, a wide range of functions

Inputs

From leadership

- Receives guidance on top business events and strategies
- Receives relevant business data for correlation

From IT

- Receives relevant business data for correlation
- Receives support for monitoring design
- Receives metrics on security controls

Outputs

To leadership

- Provides reporting on cyber risk current state
- Advises on cyber threats that may impact the business

To IT

- Provides threat insights to inform technology controls
- Provides requirements for solution design

Architecture and engineering

IT operations

Application development

Other IT functions

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

Deloitte.
University Press

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.