Deloitte.
University Press

New perspectives on how cyber risk can power performance

Cyber

Risk powers performance.

Sam Balaji
Business Leader
Global Risk Advisory

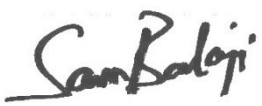
The traditional view of risk management solely as a means of risk avoidance is changing. Perhaps, it's time to raise the possibility that risk is something we not only *should* accept, but embrace. This includes cyber risk. Reports of cyber breaches and attacks surface with alarming regularity. These 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
Business Leader
Global Risk Advisory

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.

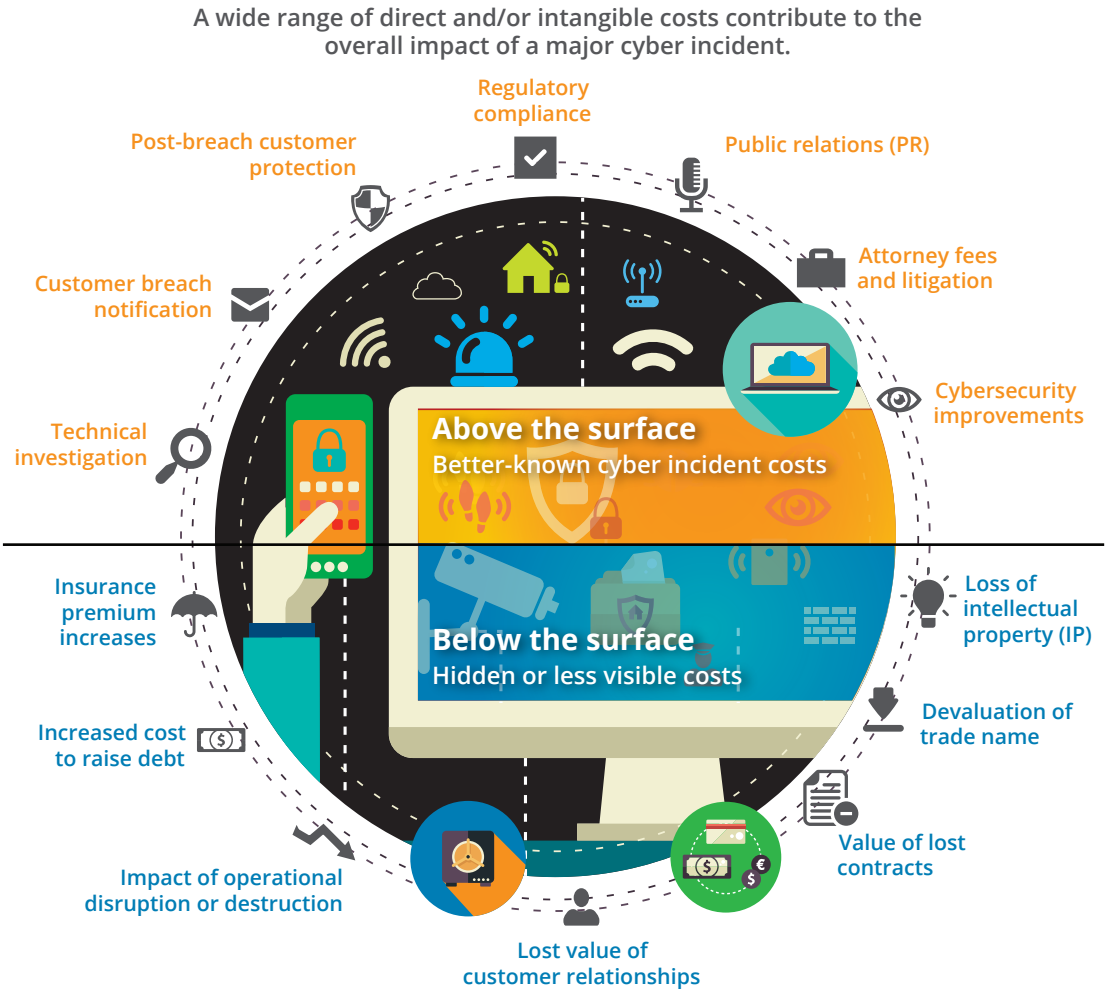
What assets are most at risk? Naturally, thieves are primarily after corporate secrets, rather than IP already in the public domain, such as patents and trademarks. Most valuable to perpetrators are trade secrets and proprietary business information that can be monetized quickly. Trade secrets can include 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.

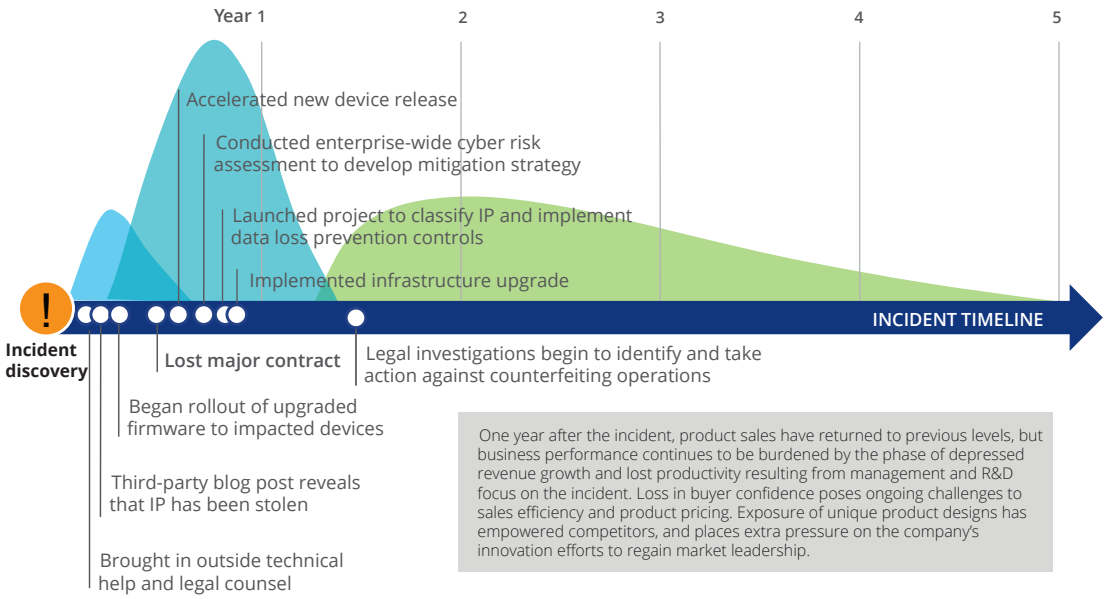
During the initial triage phase, Thing to Thing hires big guns from a top PR firm to reach out to stakeholders and create a face-saving public image campaign. In addition, the company retains attorneys and a forensics firm to investigate the event, and a cybersecurity firm to help triage and remediate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

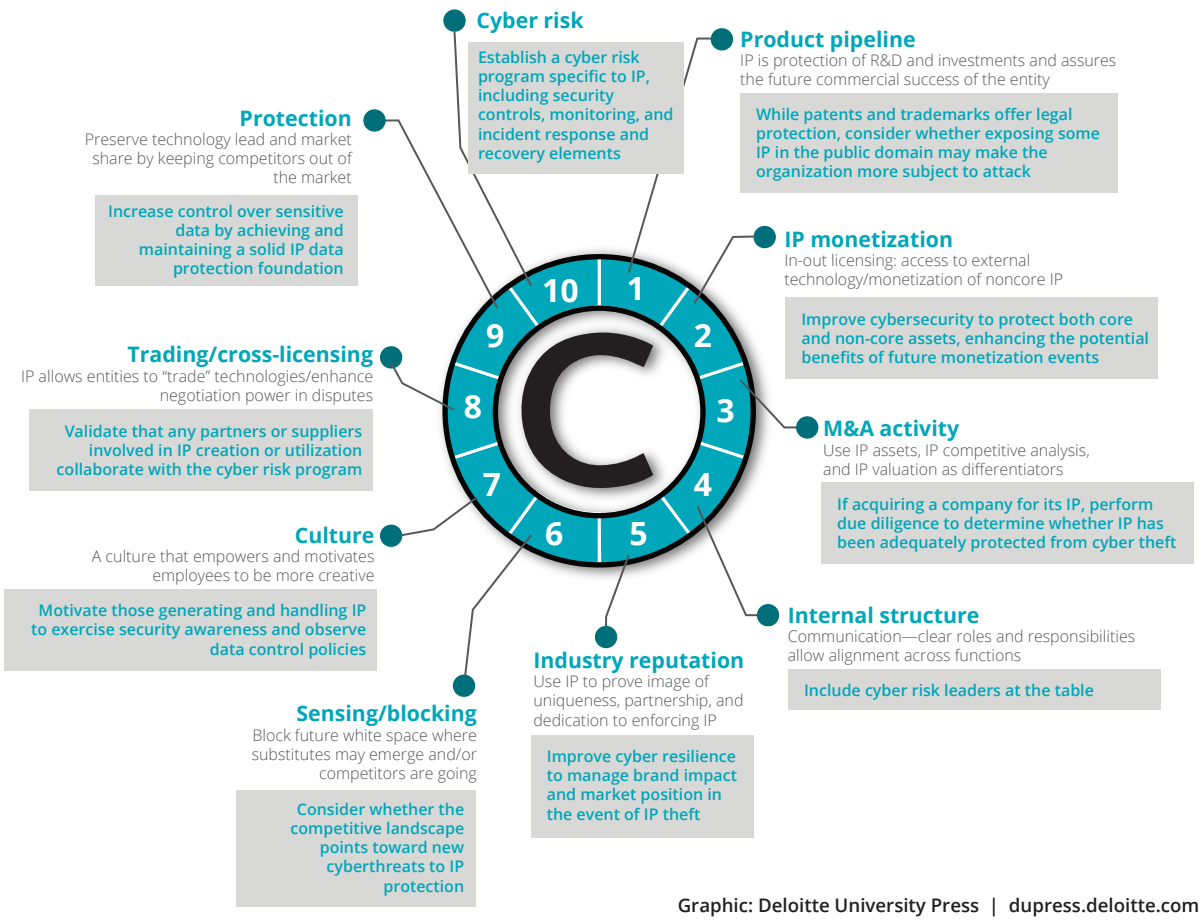
THE goal of the scenario above is not to shock with alarmingly high figures but, rather, to highlight the impacts that matter most in the aftermath of a cyber breach so that executives can understand the full ramifications of IP theft. Once executives realize the importance of protecting digital IP, 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.

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