Deloitte.

Beneath the surface of a cyberattack

A deeper look at business impacts

Cyber

Foreword

In our work and conversations with more than a thousand clients across virtually all industry sectors, we consistently hear that boards, executive management, and technology leaders are struggling to connect the dots on a wide range of topics familiarly grouped under the heading of "cyber." At the core of this struggle is a view that business executives and security professionals seldom speak the same language and—perhaps more important—they rarely approach cyber challenges in a way that integrates multiple competencies to create better business context and insight in their cyber strategies.

We have found this to be especially true in the estimation of risks and financial impact associated with cyberattacks. In particular, traditional approaches to calculating impacts of cyber incidents have focused largely on the direct costs associated with the theft of personal information. While this is helpful in certain situations, it does not account for the growing number and severity of incidents that do not necessarily involve the breach of customer or employee records—for example, the theft of intellectual property, the disruption of core operations, or the destruction of critical infrastructure. This focus on personal information is partly due to the availability of data, but it is also due to a tendency to emphasize the impacts that are visible and easiest to quantify.

In order to provide a more complete view of the immediate and longer-term business impacts of cyber incidents, Deloitte Advisory has brought together our market leading Cyber Risk, Forensic & Investigation, and Valuation teams—supported by our industry practices—to demonstrate how a multidisciplinary approach can yield richer business insight into any organization's cyber challenges.

In *Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts*, we have leveraged our experience with a variety of cyber incidents and our deep industry knowledge to illustrate how 14 impact factors—including many that are not often visible—can affect an organization in the days, months, and years following a cyberattack. Using financial modeling, damages quantification, and business and asset valuation techniques, we have developed approaches and guidance for estimating both the direct and intangible costs associated with these impact factors. The resulting data is intended to provide greater clarity around the potential range and financial risks associated with these factors.

This integration of cyber and valuation disciplines provides fuller insight that should inform the way organizations think about and plan for cyber incidents. It also reveals some important observations that are difficult to see through the traditional lens of direct cost—and hopefully will encourage organizations to think beyond the "conventional wisdom."

Edward W. Powers
National Managing Principal
Cyber Risk Services
Deloitte Advisory
Deloitte & Touche LLP

J. Donald Fancher
National Managing Principal
Forensic & Investigation Services
Deloitte Advisory
Deloitte Transactions and Business Analytics LLP

Justin Silber
National Managing Principal
Valuation Services
Deloitte Advisory
Deloitte Financial Advisory Services LLP

Contents

Introduction

A fundamental shift is occurring in the management of cyber risk. The idea that cyberattacks are increasingly likely—and perhaps inevitable—is beginning to take hold among executives and boards. Business leaders are realizing that we have interconnected our world mostly using technologies designed for sharing information, not protecting it. They recognize that they have to trust people—their own employees and the third parties they do business with—to handle sensitive information and operate critical infrastructure. And more and more they see that the intimate connection between their strategic agenda and the creation of cyber risk makes it infeasible for them to lock everything down and always put security first.

As a result, many organizations are beginning to adopt what Deloitte calls a *Secure.Vigilant.Resilient.*™ approach[1] to cyber risk, which appropriately balances investments in cybersecurity with efforts to develop better threat visibility, and the ability to respond more rapidly and more effectively in the event of a cyber incident. In order to prioritize properly, organizations should understand the types of cyber risk they face and be able to gauge their relative likelihood. And just as important, they need to understand the business impacts those risks are likely to involve.

A significant challenge, however, is that common perceptions about the impact of cyberattacks are mostly shaped by what companies are required to report publicly—primarily theft of personally identifiable information (PII), payment data, and personal health information (PHI). Discussions tend to focus on costs related to customer notification, credit monitoring, and the possibility of legal judgments or regulatory penalties. Important work has been done in this area, and the industry is generally converging on the calculation of a "cost per record" for consumer data breaches.[2]

The costs commonly associated with data breaches are only the most widely understood impacts, the damage seen above the surface. But theft of PII is not always an attacker's objective. Rarely brought into full view are cases of intellectual property (IP) theft, espionage, data destruction, attacks on core operations, or attempts to disable critical infrastructure. Beneath the surface, these attacks can have a much more significant impact on organizations. But the tolls they take are not broadly understood and are much more difficult to quantify.

Organizations can understand these less obvious impacts, though, by employing a multidisciplinary approach that integrates deep knowledge of cyber incidents with business context, valuation techniques, and financial quantification. With better visibility into a broader range of the potential business impacts, leaders can transform the way they manage cyber risk and improve their ability to recover when a cyberattack occurs.

Understanding impacts

Impact factors and the phases of incident response

There are many ways a cyberattack can affect an organization, and the impacts will vary depending on the nature and severity of the attack. In general, there are 14 "impact factors" that business leaders should consider when preparing for cyber incidents (see illustration on page 3). Some are well-known, direct costs commonly associated with cyber breaches; others are more far-reaching, intangible costs that are both more difficult to quantify and often hidden from public view.

These impact factors play out across an incident response lifecycle that can be broken down into three phases, which usually overlap one another and can extend differently over time, depending on the type of attack. Some of the impact factors are typically associated with one of the three phases and may represent one-time costs, such as regulatory fines. Other impact factors, such as legal costs or damages from IP loss, recur or are present throughout the recovery process.

Illustrating cyberattack impacts over time

To show how impact factors can play out when an actual attack occurs, the next sections present two scenarios—one featuring a health insurer, the other a technology company. The companies and the situations are fictitious, but the illustrations approximate how a stream of events might unfold and the effects they can have—both the familiar and the lesser-known consequences.

Understanding the cyber risk of an organization requires knowledge of the business models, operational processes, trends, maturity levels, and vulnerabilities specific to that organization and generally present in its industry sector. The scenarios, therefore, were constructed from Deloitte's deep and broad knowledge of the industries to which the fictitious companies belong.

In addition to a brief company profile and description of a cyberattack, each scenario contains a Cyber Incident Response timeline. The timeline illustrates some of the major events and developments that may occur over a five-year period, which require both business and technical responses. It also depicts the duration of the three incident response phases and approximates the relative magnitude of their business impact. A summary table for each scenario shows the estimated financial impact and approximate duration for each of the 14 impact factors.

Incident response lifecycle

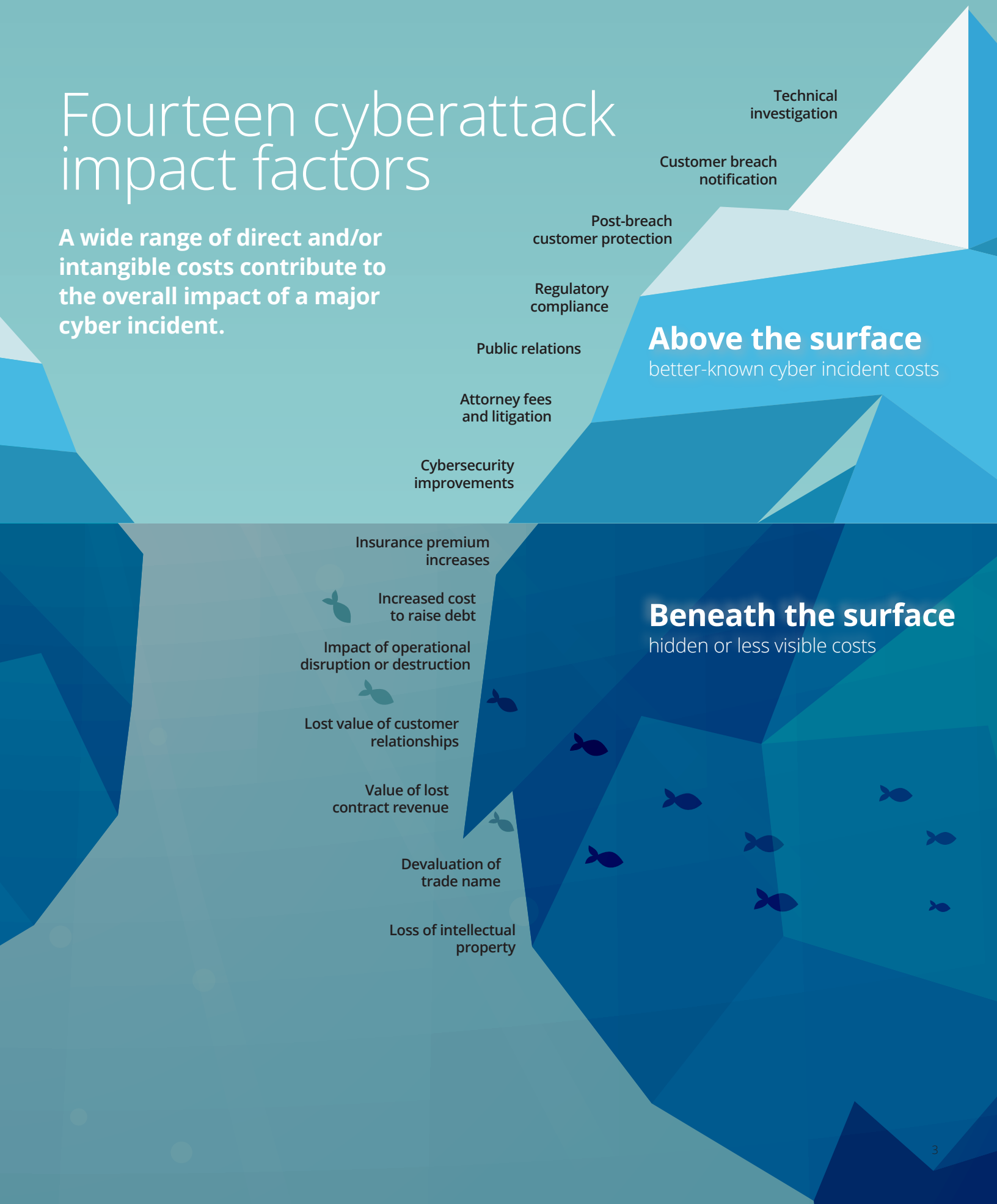
Incident triage is the highly reactive phase in the days or weeks after an attack is discovered. During this phase, business leaders direct near-term decisions and actions, including communication with external parties and formulation of strategies for continuity of important operations, if disruption has occurred. It includes the analysis of what occurred, immediate steps to stop compromises in progress, and emergency review and remediation of security controls.

Impact management involves the reactive efforts required in the weeks or months after an attack to reduce and address the direct consequences of the incident. Work streams can vary widely depending on the nature of the attack, but might include efforts to stand up interim infrastructure and adjust operational processes; reduce damage to client, customer and partner relationships; engage in cyber audit processes and respond to findings; and initiate or respond to legal or law enforcement matters.

Business recovery is the remediation phase lasting months or years when attention turns toward repairing damage to the business and preventing the occurrence of a similar event in the future. Business recovery activity is also highly variable, but can include the rebuilding or redesign of business processes, systems, applications, or other assets; the development of strategies to rebuild reputation, revenue streams, and competitive advantage; investment in security improvements, detection systems, or preparedness capabilities—all with the goal of emerging from the crisis stronger than before.

Fourteen cyberattack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident.



Calculating impacts

Each of the 14 impact factors requires a specific approach for estimating cost. The illustration on page 3 shows that "above the surface" are many tangible, direct costs. These factors, generally well-understood, include such things as costs to notify customers or provide personal credit protection. They are relatively straightforward to approximate using a combination of profile information for each company, publicly available data, and cost assumptions derived from industry and market research. These assumptions are detailed in the appendix.

"Beneath the surface," however, many of the impacts are intangible and more difficult to quantify, including costs associated with loss of IP or contracts, credit rating impact, or damage to the value of a trade name. In situations where intangible assets are at risk, impact can be estimated using generally accepted standard financial measures, damage quantification methodologies, and valuation methods. The sidebar titled "Assigning Value to Intangible Losses" explains some of the underlying concepts for how impacts were analyzed in these categories. Further detail is provided in the appendix.

Of course, a shift in the way the company was modeled or in the assumptions regarding the incident and the response could influence the analysis, leading to change in the potential financial impact. Furthermore, it is important to note that in some cyber incidents, all 14 impact factors will be felt; others may involve many, but not all. During Deloitte's scenario calculation and financial analysis process, care was taken to account for each financial impact only once.

And finally, as those familiar with financial valuation techniques are aware, company values are typically modeled in perpetuity or extrapolated for an indefinite time period. However, our work quantifies the present value of the economic impact over a five-year period to demonstrate and account for a company's ability to recover and mitigate damages resulting from a cyberattack.

Assigning value to intangible losses

Various financial modeling techniques were used to estimate the value of lost IP, damage to trade name, and impact of lost customer relationships and contracts. The following concepts are useful in understanding these methods.

Valuation and financial quantification are associated with a specific point in time

Given the time value of money and a wide range of unforeseen internal and external factors that may also impact the future value of an asset, the aim of the valuation process is to assign an estimated value or financial benefit to an asset at a specific point in time—in this case, the time the cyberattack was discovered. We applied the widely accepted Discounted Cash Flow Method under the Income Approach, which broadly entails estimating the present value of the projected economic benefits to be derived from the use of the asset.

With-and-without method

The "with-and-without" method is a comparative business valuation technique that involves estimating the value of an asset under two scenarios: one, with a certain asset or situation in place (the "situation," in this context, being the occurrence of a cyberattack); and the other without the asset or situation in place (in this case, the absence of a cyberattack). The difference in these value estimates yields the isolated value impact that can be attributed to the situation.

Reliance on assumptions

Performing a valuation or damages/loss exercise often requires the use of professional judgment and reasonable assumptions in the absence of detailed, actual data. In our analysis of the impact of a cyber incident on particular assets in each of our hypothetical scenarios, we used typical industry benchmarks (or conducted research to identify benchmarks) to arrive at assumptions for a financial impact analysis. Some of these assumptions leverage Deloitte's wealth of experience performing valuations and damages analyses in similar contexts, as well as broad practical knowledge of the industries represented in the scenarios.

Scenario A: US health insurer

About the company

- $60 billion annual revenue
- 50,000 employees
- 23.5 million members across the US (60 percent subscribed through employer contracts)
- Uses a patient care application, which provides medical alerts and allows health practitioners across its provider network to access patient records and insurance coverage information
- Holds open enrollment (the annual period when people can enroll in health insurance plans) November through January
- Regulated by both state and federal authorities
- Plans to raise $1 billion in debt capital to acquire a health system
- Pays $7 million annual premium for a $100 million cyber insurance policy

The cyber incident

In May, the company learned that a laptop containing 2.8 million of its personal health information (PHI) records had been stolen from the company's health care analytics software vendor. The compromise was revealed five days later when the company was notified by a corporate client that information associated with some of the client's employees had been listed for sale on cybercrime "dark web" sites. Concurrently, administrators of the patient care application began to notice a significant increase in the number of new user accounts created and in active use. They also detected that an additional one million patient records had been downloaded from the application database and were unable to confirm it was for authorized use. As a result, the company shut down physician access to the patient care application and activated its cyber incident response team. The application was kept offline for two weeks while the incident was investigated. During this time, coverage and claims validation between the company and its physicians and providers had to be done manually, requiring help from a professional services organization to provide "surge support" in the company's call center. Technical investigation revealed that cyberattackers had gained access to the patient care application using privileged credentials from the stolen laptop and had created a significant number of user IDs. Consequently, before service could be restored, new user accounts had to be issued for all application users, and new application and system controls were put in place.

The aftermath

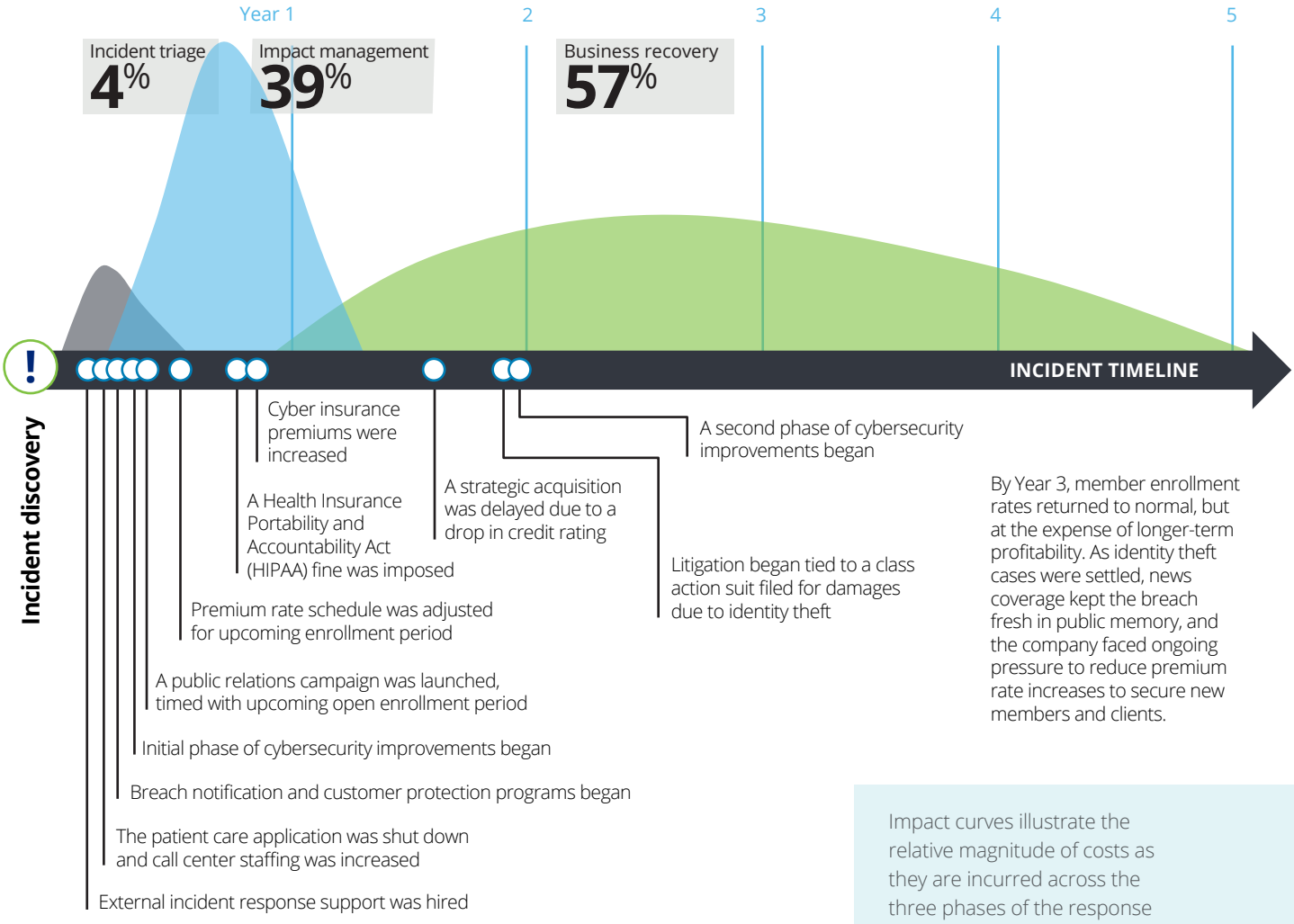
In the short term, core business functions were disrupted by the shutdown of physician access to the patient care application. While the application was unavailable, physicians and providers relied on less effective and efficient means of receiving medical alerts, increasing risk to patients. Without full access to health insurance coverage information, physicians and providers could not be certain of the financial implications—to both their institution and their patients—associated with the choice of care they provided.

As the incident unfolded, impact to reputation and damage to trade name mounted. Lack of confidence in the company's data protection practices resulted in the loss of customers for approximately three years as some corporate clients and individual subscribers chose other health plan alternatives. Higher borrowing costs resulted in the delay of a strategic acquisition and, most impactful, the incident forced the company to mitigate reputation damage and member loss by reducing its annual premium increase over a five-year period. The company faced ongoing scrutiny for its handling of the incident; many months after the breach their cyber insurance premiums were raised and legal fees accumulated as the company faced identity theft lawsuits.

Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Post-breach customer protection	3 years	21.00	1.25%
	Cybersecurity improvements	1 year	14.00	0.83%
	Customer breach notification	6 months	10.00	0.60%
	Attorney fees and litigation	5 years	10.00	0.60%
	Regulatory compliance (HIPAA fines)	1 year	2.00	0.12%
	Public relations	1 year	1.00	0.06%
	Technical investigation	6 weeks	1.00	0.06%
Beneath the surface	Value of lost contract revenue (premiums)	5 years	830.00	49.43%
	Lost value of customer relationships (members)	3 years	430.00	25.61%
	Devaluation of trade name	5 years	230.00	13.70%
	Increased cost to raise debt	5 years	60.00	3.57%
	Insurance premium increases	3 years	40.00	2.38%
	Operational disruption	Immediate	30.00	1.79%
	Loss of intellectual property	Not applicable	-	0.00%
	Total		**$1,679.00**	**100.00%**

Scenario A: Cyber incident response timeline—how the events and impacts unfolded



Impact curves illustrate the relative magnitude of costs as they are incurred across the three phases of the response process, which are defined on page 2.

The timeline shows major milestone events and work efforts throughout the process. Some are externally imposed, and others reflect the actions taken in response by the company.

Highlights of the business impact

The total cost of this cyberattack was greater than $1.6 billion over a five-year timeframe, and of significant interest, only 3.5 percent of the impact was accounted for "above the surface." To the casual observer, this incident was a classic example of PHI data theft, and while the company suffered common ramifications of a data breach, including customer notification, customer protection, and regulatory fines, there were much deeper implications. In reality, over 96 percent of the impact was "beneath the surface." What's more, almost 89 percent of the impact was associated with just three "beneath the surface" impact factors: value of lost contract revenue; devaluation of trade name; and lost value of customer relationships.

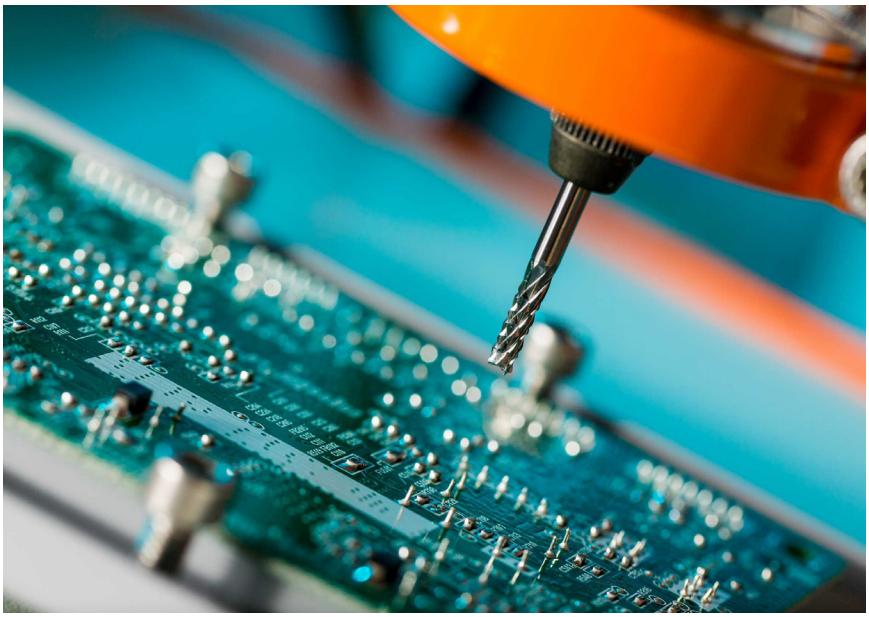
Another interesting observation is how the impact played out over time. The immediate costs to "stop the bleeding" in the triage phase accounted for less than 4 percent of overall financial impact. Impact during the impact management phase jumped to nearly 40 percent. But that meant that approximately 57 percent of the impact played out in the years following the incident, challenging thinking that the year after an incident is the most impactful. In this scenario, the largest impacts were less obvious factors that played out over time. Below is an explanation of how the three most impactful factors were estimated.

Value of lost contract revenue (premiums): In this scenario, contracts were not canceled, however, as the company looked to reduce the damage of the incident, it adjusted the premium increase they had historically charged their members. This resulted in an estimated loss of $830 million over five years. To arrive at this calculation, it was assumed that the average increase in annual premiums is reduced by 20 percent in year one and premium growth rates steadily increased to meet average growth rates, consistent with those prior to the incident, after five years.

Devaluation of trade name: Due to erosion of revenue, the company's trade name value decreased, resulting in a $230 million loss. To determine the financial impact of a cyber incident on the value of a company's trade name, the likely value of the trade name both before and after the cyberattack was assessed. To assess the trade name value in both situations, we utilized the relief-from-royalty method of valuation. After evaluating similar benchmarks for a typical company in this industry, we established a reasonable royalty rate of 2 percent. The valuation of the trade name was then derived by associating 100 percent of the company's future expected revenues associated with the trade name. The health plan's trade name prior to the incident was valued at $3.9 billion. For purposes of this exercise, it was assumed that, following the cyberattack, the company faced a 6 percent erosion of revenue, defined as a combination of lost premium revenue and lost members over the course of five years. As a result, the company's trade name value potentially decreased to $3.7 billion.

Lost value of customer relationships: The decline in annual revenues due to lost members or customers caused the value of customer relationships to decline by $430 million. This calculation assumed attrition for existing customers (normally 7 percent) increased by approximately 30 percent (to 9 percent) in year one. The model also assumed that customer attrition decreased over time, and returned to a normal attrition rate of 7 percent at the end of three years.

Further, this calculation assumed new members in year one (immediately after the breach) decreased by 50 percent. However, the growth rate for new members steadily increased to normal growth rates, so that in years four and five, growth rates of 25 percent and 30 percent, respectively, were reached. Prior to the cyberattack, the total value of the company's customer relationships, or its members, was estimated at $10.3 billion. Based on the decline in annual revenues due to lost members or customers, as modeled over the five-year period, the value of customer relationships declined to $9.5 billion. This loss was in addition to the lost contract revenue (premiums) referenced above.



Scenario B: US technology manufacturer

About the company

- $40 billion annual revenue
- 60,000 employees
- Growth strategy rests on innovation to support the management of Internet of Things (IoT) environments
- Holds hundreds of contracts with clients across multiple industries, including several very large federal government contracts
- Operating profit margin prior to the incident is 12.2 percent
- Pays $3.75 million annually for $150 million in cyber insurance

The cyber incident

After significant research, development, production, and marketing, the company was six months from a major release of a core product line that supports IoT environments. Earlier versions were deployed in the field for over 12 months across the government, transportation, utilities, smart home, and smart city sectors, and among service providers who support customers in those sectors. The company was informed by a federal agency that the company's infrastructure was breached by a foreign nation-state. An investigation revealed exfiltration of IP related to multiple product lines and confirmed that 15 of the company's 30 device product lines were impacted. Revenue associated with impacted product lines was projected to be 25 percent of total revenue over the following five years. Despite efforts to keep the incident confidential, 30 days after discovery a tech blog revealed that the foreign entity may be reverse-engineering the company's IoT products.

The aftermath

The adversary's full intent was not known, but the company was concerned that counterfeit products could directly impact long-term sales and margins. It was equally concerned that attackers would exploit product vulnerabilities, or implant malicious code into their products. To be associated with future customer security incidents could be devastating to the company's reputation.

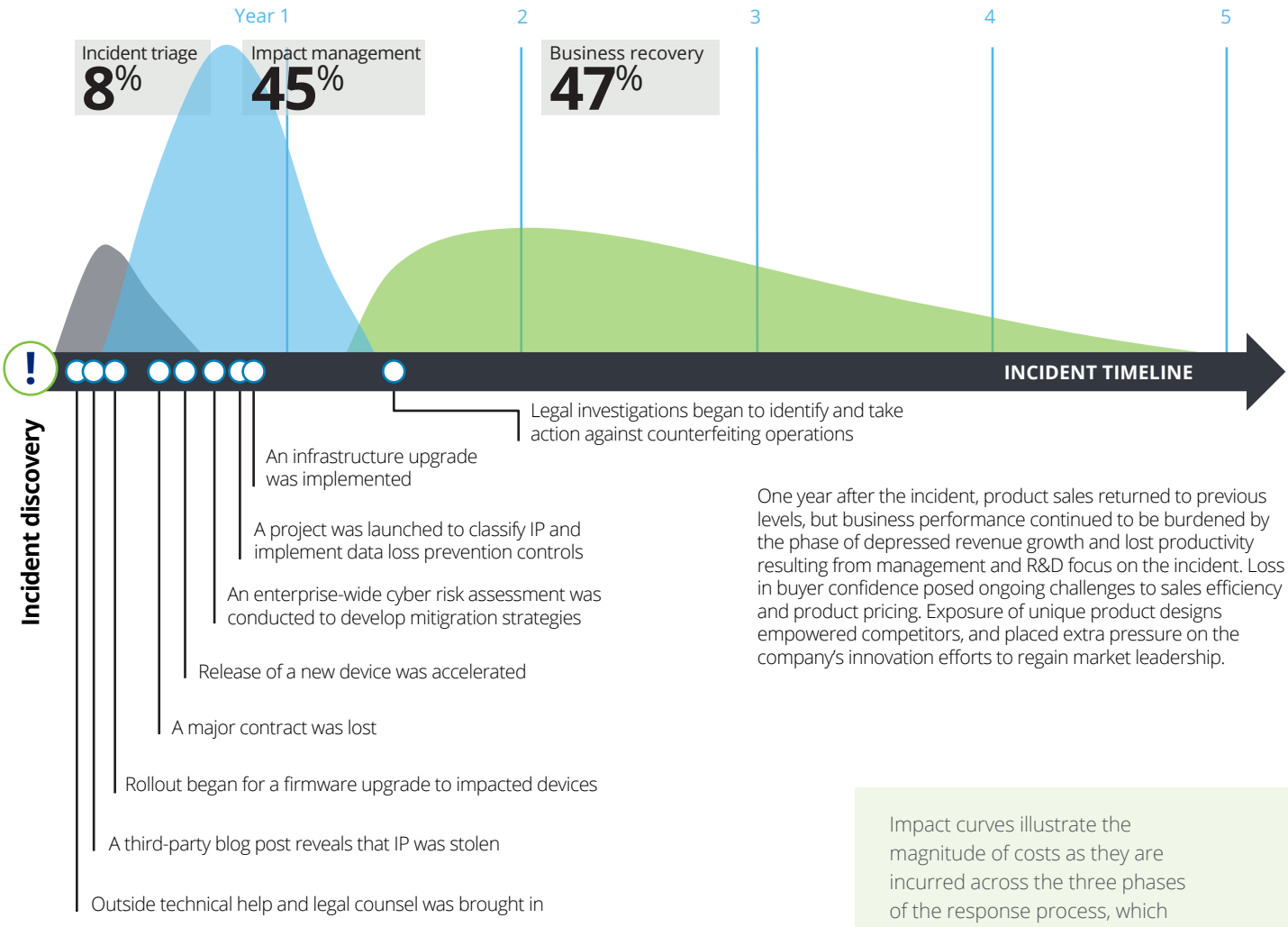
While the company was largely able to recover within five years, the incident had a number of serious consequences. Sales and shipment of affected products were suspended for four months while security vulnerabilities were addressed. When word of the incident surfaced, a large government contract was terminated, causing an additional 5 percent drop in revenue. Significant unplanned costs were incurred, including costs to redesign security features and firmware for many product lines, and to redesign future products to embed advanced anti-counterfeiting software and hardware.

The loss of IP related to multiple product lines was a significant blow to the organization and required unanticipated research and development (R&D) expenditures and product fixes. It was a full year before product sales returned to normal. Loss in market confidence lead to abnormally high sales force turnover. This type of business disruption across multiple functions caused a significant decline in operating efficiency. To help prevent future incidents, the company made security improvements to its corporate environment a top priority, including infrastructure upgrades and a data loss prevention program.

Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Cybersecurity improvements	1 year	13.00	0.40%
	Attorney fees and litigation	5 years	11.00	0.35%
	Public relations	1 year	1.00	0.03%
	Technical investigation	9 weeks	1.00	0.03%
	Customer breach notification	Not applicable	-	0.00%
	Post-breach customer protection	Not applicable	-	0.00%
	Regulatory compliance	Not applicable	-	0.00%
Beneath the surface	Value of lost contract revenue	5 years	1,600.00	49.11%
	Operational disruption	2 years	1,200.00	36.83%
	Devaluation of trade name	5 years	280.00	8.59%
	Loss of intellectual property	5 years	151.00	4.63%
	Insurance premium increases	1 year	1.00	0.03%
	Increased cost to raise debt	Not applicable	-	0.00%
	Lost value of customer relationships	Not applicable	-	0.00%
	Total		**$3,258.00**	**100.00%**

Scenario B: Cyber incident response timeline—how the events and impacts unfolded



One year after the incident, product sales returned to previous levels, but business performance continued to be burdened by the phase of depressed revenue growth and lost productivity resulting from management and R&D focus on the incident. Loss in buyer confidence posed ongoing challenges to sales efficiency and product pricing. Exposure of unique product designs empowered competitors, and placed extra pressure on the company's innovation efforts to regain market leadership.

Impact curves illustrate the magnitude of costs as they are incurred across the three phases of the response process, which are defined on page 2.

The timeline shows major milestone events and work efforts throughout the process. Some are externally imposed, and others reflect the actions taken in response by the company.

Highlights of the business impact

In this incident, which could be categorized as a case of IP theft, the overall damage across all impact factors exceeded $3.2 billion over a five-year timeframe. Notably, the vast portion of the impacts were "beneath the surface;" those "above the surface" accounted for less than 1 percent of the total. In fact, 99 percent of the impact was focused in four areas: devaluation of trade name; value of lost contract revenue; operational disruption; and loss of IP.

In terms of how the impacts played out over time, only 8 percent of the total impact fell within incident triage. Over 40 percent occurred during impact management, when operational disruption implications peaked, contract loss kicked in, and the company started to see the impact of lost IP. Interestingly, the largest impact was felt during business recovery, with half of the total impact having occurred more than two years following the incident.

Below is an explanation of how the most significant impact factors were estimated.

Devaluation of trade name: Due to the loss of intellectual property and intangible assets, and the resulting impact to its reputation, the company lost almost $280 million in the value of its trade name. Utilizing the relief-from-royalty method, a royalty rate of 1.5 percent was used to make this calculation, based on a review of comparable license agreements of similar companies, and typical profit margins of public technology hardware companies. Additionally, it was assumed that the incident continued to impact the company for five years. The company's trade name prior to the incident was valued at $1.8 billion; after the incident it was valued at $1.5 billion.

Value of lost contract revenue: As a result of the cyber breach, there would be a high probability that a significant federal contract would be cancelled, leading to an estimated loss of $1.6 billion. Though its revenue base was spread across hundreds of clients, this company was especially reliant on large contracts with federal agencies and telecommunications providers. One of these was a five-year contract with the federal government that made up 5 percent of the company's total annual revenue. The loss of this contract reduced total annual revenue by 5 percent and profit margin declined by 2 percent. With the decline in revenue, the company then functioned under a lower operating base since its fixed costs were spread over a lower revenue base.

Operational disruption: The cyberattack caused disruption to business operations, leading to $1.2 billion in losses associated with a drop in productivity. In the wake of the incident, not only did the company have to halt sales and shipments for four months, it also experienced unanticipated R&D costs; because IP had been stolen and a competitor likely could have replicated the same capabilities and functionalities, the company re-evaluated 15 product lines. Resources were re-allocated to focus on fixes to product lines, along with the redesign and implementation of security features and other cybersecurity improvement costs. Loss of sales force was also an unexpected impact in the year following the incident due to a loss in market confidence. In order to quantify the financial impact of this disruption, an overall impact to profitability was estimated before and after the cyber incident. The company would have had a profit margin of 12.2 percent and generated overall operating profits of almost $4.9 billion annually before the incident. Assuming the company's profit margin drops to 9.2 percent after the incident as a result of the disruption, its operating profit dropped to less than $3.7 billion, resulting in a $1.2 billion loss in operating profits.

Loss of IP: Within the context of this IP theft incident, the actual value of the lost IP was a significant component of the overall impact, leading to the loss of over $150 million. The company's performance and market share rested largely on the value of its proprietary technology and trade secrets. To calculate the value of this loss, the company's IP was assumed to have had a useful life of five years, and it was known that 25 percent of the company's revenue was attributable to the impacted product lines. By analyzing comparable license agreements for related technologies, and profit margins of public technology hardware companies, a royalty rate of 2.5 percent was established and used in a relief-from-royalty calculation. Based on the risks associated with IP of this nature, a discount rate of 12 percent was used. Applying values to the IP both before and after the cyber event, the loss of IP cost the company over $150 million.

Scenario takeaways

For all the attention that major breaches receive, business leaders rarely see what occurs behind the walls of an organization struggling to recover from an attack—until it happens to them. Our intent is to help leaders broaden their understanding of the potential consequences of an enterprise cyber incident. With a more robust picture of how an incident may play out and what may be at stake, leaders may be better informed on how to frame a risk-based approach and sharpen the focus of limited resources to enhance security, vigilance, and resilience in those areas of the enterprise that may lead to the greatest impacts. This focus ultimately allows leaders to improve the organization's ability to thrive in the face of today's environment, where cyberattacks are prevalent.

The scenarios outlined represent different industries and attack objectives and illustrate two examples of the many ways a cyberattack can unfold. Though necessarily simplified for this effort, the scenarios demonstrate the unique ways the defined impact factors play out based on the company, the incident, and the response. In sum, the examples highlight that a cyberattack may include a broader set of business impacts than typically considered, and that addressing these impacts may be highly complex and, in some cases, more costly than cyberattack impacts "above the surface."

In comparing the scenarios, several over-arching conclusions stand out.

"Above the surface" costs commonly associated with data breaches may only be the tip of the iceberg and are relatively small compared with the overall impacts.

Scenario A shows that even in an attack involving typical data theft, the classic "above the surface" costs associated with data breach response may not be the most significant over the course of the incident.

The impact of a cyberattack plays out over years following an incident.

The immediate triage phase is costly, but the long-term efforts may take a far greater toll. Long after intruders are removed and public scrutiny has faded, the impacts from a cyberattack can reverberate over a multi-year timeline. Legal costs can cascade as stolen data is leveraged in various ways over time; it can take years to recover pre-incident growth and profitability levels; and brand impact can play out in multiple ways.

Recovering from an attack is not just a technical effort.

Although cyberattacks are conducted through technology-based means and can cause very significant damage to infrastructure, equipment and applications, the major damage will usually be to business value, not to IT assets themselves. Incident response is not primarily a technical effort. As the scenarios demonstrate, the technical work to investigate, analyze, clean, and repair computer systems is soon overshadowed by efforts to manage customer and third-party relationships, legal matters, investment decisions, and changes in strategic course, which are significant business leadership activities.

Going forward

What you do matters

Although cyberattacks are all but inevitable, the extent of their damage is not. There are actions that our scenario companies took—or could have taken—that may have changed the outcome. In Scenario A, for example, we assume that the company had an integrated identity and access management system; therefore, user account changes could be implemented in a matter of weeks versus months. Furthermore, had the cyberattack occurred closer to open enrollment, news of a data breach might have had a more devastating impact on subscriber rates; in that case, swift and decisive public relations and customer care action to reduce damage would have been especially urgent. An additional angle is the role of the analytics vendor, who promptly reported that a laptop with the insurer's data had been stolen. The resulting impacts may have turned out differently if the vendor had not reported the loss so promptly or if data residing on that laptop had been properly encrypted.

In the case of the technology company, perhaps additional investments in cyber risk monitoring could have enabled the detection of an early-stage infiltration before attackers were able to confiscate IP. As the scenario implies, better governance around sensitive IP might have narrowed the range of what could be accessed when attackers did succeed in gaining access to the network. Furthermore, while hoping that news of the theft would not go public, the organization could have taken more proactive steps in managing the relationships and communications with its largest customers to avoid an impactful contract termination.

Becoming more resilient

For many organizations, becoming truly resilient to cyberattacks calls for a shift in mindset that changes how they perceive cyber risk and potential impacts. It requires organizational transformation that broadens the scope of involvement at the top of the organization and instills focus on business risk, not just technology controls. It involves the ability to reprioritize and refocus investments on mitigating likely outcomes, based on a broad understanding of attackers' motives and the ability to anticipate high-impact scenarios. Many will find the following to be useful first steps.

Convene the right team.

Evaluate organizational readiness by bringing together the right business and technical leaders to develop a list of high-risk cyberattack scenarios. This will likely require a team that collectively understands business strategy, products, revenue streams, operations, technology, regulation and, of course, the organization's cyber risk program.

Identify top risk areas and assets.

In some enterprises, particular data sets, computer systems, control devices, or other digital assets represent high value unto themselves. In many cases, the value of information and technology assets is tied to the criticality of the business processes and relationships they enable. Once those processes and activities are identified, it is important to understand the underlying technical environment, model the threats to the environment, and draw a realistic picture of the direct and intangible business impacts should they be compromised. The lens should not be focused too narrowly on data theft; other possible attack scenarios should be considered.

"Right-size" spend to reduce incident impact.

Budgets will never be big enough if the aim is to try to prevent every possible incident. While greater investment may be required, it is likely more important to invest in a more risk-focused manner. Effort should be taken to define the organization's top risk areas and assets and model realistic attack scenarios. This enables an organization to establish a reasonable level of investment in various areas of a cyber risk program.

Modernize what "readiness" means.

An incident response plan, if built on narrow assumptions, is likely to fall short at a time of crisis. With awareness of what matters most to the organization, plans can be made to involve the various parties needed to protect, defend, and recover if those things are compromised. Incident response plans can be appropriately broadened—and rehearsed—to anticipate and prepare for the high-risk cyberattack scenarios identified. Establishing broad cyber-awareness and engagement across the organization improves the ability to collaborate and react when the cyber incident alarm rings.

Do more than prepare.

Cyber readiness is not just about what happens after an attack. Right now, malware is sitting undetected on networked systems within an organization or on the devices of partners, vendors, or employees. There may be ill-intended users within the walls of the company who could use authorized access to inflict damage. In some areas, tighter security practices may be warranted. Other areas may be technically impossible or impractical to secure further, but might warrant stronger capabilities to detect potentially malicious activity. Every organization should institute some variation of a secure, vigilant, and resilient approach that is aligned to its cyber risk posture and program.

Bringing cyber impacts to the surface

Beneath the surface of a cyberattack is intended to shed light on a broad set of business impacts that are overlooked in most conversations about cyber risk. Cyber incidents may begin as a technology issue, but they typically extend well beyond the technology domain. These events can hit at the very heart of business value and performance.

We have attempted to demonstrate the toll cyber incidents can have on enterprise performance far beyond the considerations usually associated with data breaches.

Whether adversaries set their sights on IP, trade secrets, operational disruption, fraud, or data records, cyberattacks can have deep and long-lasting effects on an organization.

We encourage readers to challenge common assumptions about the breadth, depth, and duration of cyber incidents and to take a more comprehensive view of their potential cost. By viewing cyber risk through this wider lens, we believe that organizations can ultimately improve their ability to survive and thrive in the face of increasingly likely cyberattacks.

Endnotes

1. For a discussion of Deloitte's *Secure.Vigilant.Resilient.* approach, see *Changing the Game on Cyber Risk: The Imperative to be Secure, Vigilant, and Resilient*, Deloitte Development LLC, 2015.
2. Ponemon Institute is recognized as a leader in this area for its widely referenced annual *Cost of a Data Breach* studies, available at www.ponemon.org.
3. Projected net cash flows over the five-year period were reflected in present terms to reflect the time value of money and risk associated with obtaining these cash flows in the future.
4. Operational efficiency is measured by the median operating profit margin of guideline public companies in the technology industry, based on data from S&P Capital IQ.
5. Zurich Insurance Company, *The good, the bad and the careless: An overview of corporate cyber risk*, December 2014.
6. Ponemon Institute, *2015 Cost of a Data Breach Study: Global Analysis*, May 2015.
7. Zurich Insurance Company, *The good, the bad and the careless: An overview of corporate cyber risk*, December 2014.
8. Ponemon Institute, *The Aftermath of a Data Breach: Consumer Sentiment*, April 2014. This report indicates that only 29 percent of customers who were offered identity theft protection following a breach actually signed up for the services.
9. CMMI is a registered trademark of Carnegie Mellon University. The CMMI model is a widely referenced framework for process and performance improvement that leverages a 0-5 benchmark scale as a basis to reflect an entity's level of process maturity.
10. Given the use of fairly recent cases, there is not enough data to ascertain impact to long-term credit rating.
11. Based on data from Morningstar Credit Ratings, http://www.morningstar.com/credit-rating/corporate.aspx.
12. Baa yield data from December 31, 2015, http://www.federalreserve.gov/releases/h15/20160104/.
13. Truven Health Analytics MarketScan® Research Databases.

Appendix

Definitions of the 14 cyberattack impact factors and how costs were developed

This appendix provides further detail on the methods used to determine scenario costs for each of the 14 impact factors. Many direct costs are generally well-understood and relatively straightforward to approximate based on publicly available information. "Assigning Value to Intangible Losses" on page 4 describes financial modeling techniques used to quantify intangible impact factors. As discussed, these techniques often require reliance on assumptions. Deloitte reviewed and analyzed data associated with cyber incidents occurring over the last few years, supplemented by insights from well-known studies conducted by other organizations, as cited. The incidents reviewed ranged from theft of high volumes of sensitive data, to theft of strategic information, to instances of severe operational disruption; some cases involved more than one attack type.

Calculation of both direct and intangible costs also requires consideration of company-specific information provided as part of the profile of each of the fictitious companies. These company profiles, as described on the scenario pages, were derived from Deloitte's broad knowledge of the specific industry sectors to which the profiled companies belong. Profiling of a plausible, fictitious company requires knowledge of the business, business trends, typical cybersecurity maturity levels, typical cyber risk vulnerabilities, revenue models, and operational processes within each industry sector. In some instances, cost estimates and related values have been simplified for illustration purposes, as presenting all underlying variables would not be feasible within the scope or length of this paper.

Although, as noted on page 4, value is estimated at a specific point in time, the term over which a company would incur tangible actual costs would vary. Some would be immediate, as in the case of the health insurer's losses associated with health claims fraud; other impact factors might be applicable over years, as in the case of the health insurance company's post-breach customer protection costs or the longer-term devaluation of the technology company's trade name.

Fourteen cyberattack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident.

Above the surface: Well-known cyber incident costs

Technical investigation

The costs associated with technical investigations are direct expenses for analysis to determine what happened during a cyber incident and who was responsible. An immediate objective is to support rapidly halting the spread of a compromise and take action to limit its impact to systems, infrastructure, and data. Efforts involve digital forensics, and malware and threat analysis to determine root cause to assist in the remediation and recovery of impacted systems, and to inform future cybersecurity improvements.

The scale of investigation activity can vary widely depending on type and complexity of the breach, and to some extent directly reflects the number of computing systems potentially impacted by the compromise. Estimated costs for this impact factor were based on Deloitte's experience in situations similar to the fictitious scenarios presented. For scenario A, investigative work would center on analysis of data within the patient care application and efforts to assess the extent of privileged account compromise. A team of five incident response specialists would likely be deployed for approximately six weeks, costing an estimated $600,000. For Scenario B, given the possible involvement of a sophisticated nation-state actor and the range of systems used to support multiple product lines, a deeper technical investigation of the broader environment would be necessary to understand the full scope and impact of the breach. This investigation is estimated to require five incident response specialists over a nine-week period, at a total estimated cost of $1,080,000.

Customer breach notification

Customer breach notification costs include the direct expenses associated with informing and advising individuals whose data has been compromised, as typically mandated by state or federal law or industry regulation. These can include printing, mailing, and call center services, among others. Deloitte has used an average indicator of $2.75 provided by Zurich Insurance stating that notification costs range between $0.50 and $5 per customer.[5] According to the Ponemon Institute, breach notification costs have recently declined somewhat.[6] Assuming that costs for these services may continue to decline over time, Deloitte has chosen to use a figure of $2.75 per stolen record.

Post-breach customer protection

Post-breach customer protection costs are direct costs associated with services to detect and protect against potential efforts to use an individual's compromised personal data for unauthorized purposes. To estimate the direct cost of credit monitoring or identify theft protection services, Deloitte used the midpoint of Zurich Insurance's guidance that typical costs range from $10 to $30 per customer for an annual subscription[7] and a Ponemon Institute study indicating that, of customers surveyed, only 9 percent actually registered for the identity theft protection services that had been offered.[8] These figures were applied to the number of customer records breached (3,800,000 in Scenario A; not applicable in Scenario B).

Above the surface: Well-known cyber incident costs

Regulatory compliance

Regulatory compliance costs are fines or fees levied as a result of non-compliance with federal or state cyber breach related laws and/or regulations. Company profiles include assumptions about which federal, local, international and/or industry regulations the company may be subject to. Costs were assigned to those factors based on publicly available information regarding fines typically imposed. Looking forward, heightened focus on breaches is triggering greater regulatory and legislative scrutiny. This is likely to complicate compliance challenges and costs at both the state and federal level—including preparing for and defending against government compliance actions.

Public relations

Public relations costs are the direct costs associated with managing external communications or brand monitoring following an incident. Deloitte surveyed leading communications firms and, based on information provided, conservatively estimates that a four-week PR campaign in the immediate aftermath of a cyber incident costs $400,000 on average. Extended campaigns to monitor and repair trade name damage were found to be conservatively estimated at $1 million per year.

Attorney fees and litigation

Attorney fees and litigation costs can encompass a wide range of legal advisory fees and settlement costs externally imposed and costs associated with legal actions the company may take to defend its interests. Such fees could potentially be offset through the recovery of damages as a result of assertive litigation pursued against an attacker, especially in regards to the theft of IP. However, the recovery could take years to pursue through litigation and may not be ultimately recoverable, even after a positive verdict in favor of the company. Based on our analysis of publicly available data pertaining to recent consumer settlement cases and other legal costs relating to cyber incidents, we observed that, on average, it could cost companies approximately $10 million in attorney fees, potential settlement of loss claims, and other legal matters. The cases surveyed include both data breaches and cyber incidents that caused operational disruption. We do note that this amount is greatly dependent on the scale, nature, and severity of the incident, and the probability of settlement, among other factors. This information was used as a basis to estimate what costs both the fictitious companies might face over a three-year period.

Cybersecurity improvements

The costs associated with cybersecurity improvements are direct expenses for technical improvements to the infrastructure, security controls, monitoring capabilities, or surrounding processes, specifically to recover business operations after an incident or to prevent a similar occurrence in the future. Estimated cost of cybersecurity improvements were based on Deloitte's experience of typical costs for the kinds of projects undertaken in each fictitious scenario. For Scenario A, these costs include efforts to restore and implement additional security controls around the claim processing system; expand vulnerability, identity and access management programs; and establish a security operations center (SOC). Cybersecurity improvements for Scenario B include an enterprise-wide cyber risk assessment; upgrades to its network infrastructure; and implementation of a data classification and data loss prevention program.

Fourteen cyberattack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident.

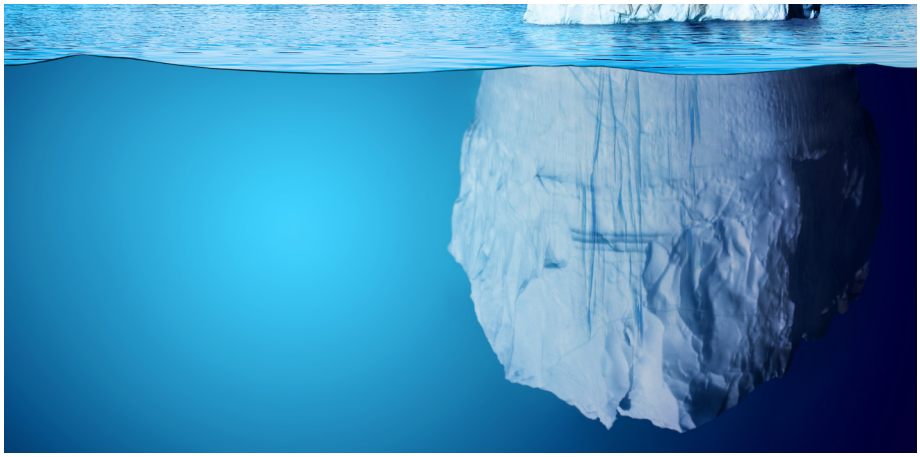
Beneath the surface: Hidden or less visible costs

Insurance premium increases

Insurance premium increases are the additional costs an insured entity might incur to purchase or renew cyber risk insurance policies following a cyber incident. There is little public data available on actual premium increases following cyberattacks. Deloitte conducted informal research among leading providers of cyber insurance and found that it is not uncommon for a policyholder to face a 200 percent increase in premiums for the same coverage, or possibly even be denied coverage until stringent conditions were met following a cyber incident. According to our sources, factors that influence future costs can include: willingness and depth of information provided by the policy holder upon review of the incident; the policy holder's plans to improve incident handling or other aspects of their security program; anticipated litigation; and assumptions concerning the company's level of cybersecurity "maturity." For purposes of this study, Deloitte assumes a premium increase of 200 percent for a company whose cyber risk program was rated at a 3.0 on a Capability Maturity Model Integration (CMMI®) scale.[9] Factored in to our company profiles were assumptions about each fictitious organization's cyber risk CMMI score. We adjusted premium increases proportionately up or down based on the company's maturity above or below that grade. For Scenario A, we assumed the company had a cyber risk program rated a 2.0 on the CMMI scale. For Scenario B, we assumed the company had a cyber risk program rated a 4.0 on the CMMI scale. Further, we assume that in many cases, by demonstrating cybersecurity program improvements, lower insurance premiums could be negotiated after a one-year period.

Increased cost to raise debt

Increased cost to raise debt occurs when, as a result of a drop in credit rating, the victim organization faces higher interest rates for borrowed capital, either when raising debt, or when renegotiating existing debt. Organizations appear to be perceived as higher-risk borrowers during the months following a cyber incident. Deloitte analyzed the credit rating of nine closely related public companies (from the same industry and comparable in size) and observed an average Standard & Poor's credit rating of A, and assessed these companies against companies which had recently suffered a cyber incident.[10] It was observed that, in the short term, the credit rating agencies typically downgrade by one level companies that have experienced a cyber incident. For purposes of establishing costs in Scenario A (this impact factor is not applicable in Scenario B), a post-cyber incident credit rating decline from A to Baa was assumed.[11] Bloomberg's median yields for a large universe of corporate bonds (a composite index) were applied. A yield for a typical 10-year, A-rated corporate bond was 3.44 percent.[12] This same median yield for a universe of Baa-rated corporate bonds was 4.48 percent, resulting in an incremental yield due to rating drop of 1.04 percent. The health plan company in Scenario A seeks to finance $1 billion over ten years for an acquisition. After suffering a cyber incident, it would cost the company $242.5 million in interest, as opposed to the $183.3 million it would have cost the company had it not sustained a cyber incident—an increased borrowing cost of $59 million over the term of the loan.



Impact of operational disruption or destruction

Impact of operational disruption or destruction is a highly variable cost category that includes losses tied to manipulation or alteration of normal business operations and costs associated with rebuilding operational capabilities. This could include the need to repair equipment and facilities, build temporary infrastructure, divert resources from one part of the business to another, or increase current resources to support alternative business operations to replace the function of systems that have been temporarily shut down; it could also include losses associated with inability to deliver goods or services. The nature of operational disruption—and therefore the appropriate method of calculating its impact—is very specific to each situation and requires direct knowledge of a number of distinct information components.

For Scenario A, calculating the financial impact of operational disruption entails estimating costs associated with hiring an external professional services organization to augment call center staffing so that coverage can be confirmed for claims submitted during the two-week triage period that the patient care application is shut down. Using data obtained from Truven Health Analytics MarketScan,[13] an analysis was run to determine, based on the average number of claims generated per member per health care visit (3.7), and the average percentage of insurance claims that are typically pre-qualified for insurance coverage (75 percent), that the temporary call center would handle almost 2.5 million claims over the two-week period, requiring over 800,000 hours of staff time and roughly 100 hours of supervisory time. This equates to approximately $27 million in personnel costs at typical hourly rates. Added to this are approximately $3 million in computing and communications infrastructure equipment and services, totaling approximately $30.0 million in operational disruption costs.

In situations such as Scenario B, a precise bottom-up calculation may be most desired, however, such an effort would require gathering a wide range of very detailed information over the duration of the actual incident response and recovery efforts, such as personnel hours spent on unplanned efforts, salary costs, impact of lost opportunity, excess R&D costs, and others. Absent such detailed information, a macro-level projection of impact to the company is often done by calculating an estimate of the decline in operating profit margin; such an effort was employed by Deloitte for this scenario. Leveraging available data on the profit margins of public companies in this industry, and assuming that this enterprise prior to the incident had a typical operational efficiency profile (equating to a 12.2 percent operating profit margin), the company would have generated overall operating profits of almost $4.9 billion annually before the incident. After the incident, the company sees a reduction in operating margin due to a loss in revenue over the same fixed costs, with the addition of cybersecurity improvement costs and additional R&D efforts. Assuming the company's profit margin drops to 9.2 percent, its operating profit drops to less than $3.7 billion, resulting in a $1.2 billion loss in operating profits.

Beneath the surface: Hidden or less visible costs

Lost value of customer relationships

During an initial triage period immediately following a breach, it can be hard to track and quantify how many customers are lost. Economists and marketing teams approach this challenge by attaching a "value" to each customer or member to quantify how much the business must invest to acquire that customer or member. They then look at the likely revenue that this one customer or member will generate for the business over time. These numbers can then be evaluated per industry and particular organization to estimate how much investment is needed to attract and acquire new customers. The value of lost customer relationships is not applicable to Scenario B because the technology company does not sell directly to individual consumers. In Scenario A, the average attrition rate of existing customers (or members) is assumed to be 7 percent. After the incident, the attrition rate for customers or members is estimated to increase by approximately 30 percent to 9.1 percent. The attrition rate is estimated to return to normal (7 percent) after three years. New member acquisition in the first year after the incident is estimated to decrease by 50 percent. We then estimated the value of customer relationships by calculating the incremental after-tax cash flows (or "excess earnings") attributable only to the customer relationships and used the with-and-without method, as described earlier, to evaluate the impact of lost customers (or members) due to a cyber incident.

Value of lost contract revenue

Value of lost contract revenue (or value of premiums, in the case of the health insurer in Scenario A) includes revenue and ultimate income loss, as well as lost future opportunity associated with contracts that are terminated as a result of a cyber incident.

To determine the financial impact of the lost contracts or premiums, Deloitte estimated the value of the contracts both before and after the cyberattack was assessed. Following a cyberattack, if the subject company were to lose contracts, we assumed there would be a decrease in revenues. We determined the present value (meaning an estimate of the value of a future income stream depicted in present dollar terms; receiving a dollar today is worth more than receiving a dollar in the future, since one could earn interest on that dollar) of cash flows that the company would earn over the term of the contracts. For Scenario A, we estimated the value of the contracts (or premiums) by calculating the incremental after-tax cash flows (or "excess earnings") attributable only to the contracts (or premiums). For Scenario B, given the size and importance of the potential lost contract to the federal government (and because for a large organization such as a federal agency, replacing a technology investment is often a time-consuming and costly endeavor), we did not assume 100 percent certainty of the loss. Instead we assumed a 50 percent likelihood of contract cancellation following the cyberattack in an effort to account for the probability of such an impactful effect occurring. The resulting probability estimate of impact to the company is a loss in value of $1.6 billion due to the cyber event. 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 $15 billion. For both scenarios, we used the with-and-without method to evaluate the impact of lost customers (e.g., members, in the case of Scenario A) due to a cyber incident over a five-year period, the period of time over which the incident is estimated to affect the company. The difference in value estimates between these two calculations yields the value eroded due to loss of the contracts or premiums.

Devaluation of trade name

Devaluation of trade name is an intangible cost category referring to the loss in value of the names, marks, or symbols an organization uses to distinguish its products and services. A brand name is associated with the name of a specific company or a specific product, whereas a trade name relates to an organization as a whole. To determine the financial impact of a cyber incident on the value of a company's trade name, the likely value of the trade name both before and after the cyber incident was assessed. To value the trade name itself, Deloitte employed the relief-from-royalty method. The relief-from-royalty method, commonly used to value IP assets such as trade names, estimates the value by analyzing what another entity would have to pay to license the company's trade name. Our analysis involved establishing a reasonable "royalty fee" by looking at royalty fees or rates paid in actual royalty transactions for similar types of IP, and the analysis of profit margins across the industries to which our fictitious companies belong, to determine what a typical company in the industry would have the capacity to pay. Using this data, Deloitte calculated the royalty rate for the health plan company in Scenario A to be 2 percent, and 1.5 percent for the technology company in Scenario B. The value of the trade name at the time of the cyber incident (using present-value calculations) was then derived by applying the royalty rate to each company's future revenues (tax-adjusted) over time.

Loss of intellectual property (IP)

Loss of IP is an intangible cost associated with loss of exclusive control over trade secrets, copyrights, investment plans, and other proprietary and confidential information, which can lead to loss of competitive advantage, loss of revenue, and lasting and potentially irreparable economic damage to the company. Types of IP include, but are not limited to, patents, designs, copyrights, trademarks, and trade secrets.

In the case of the technology company in Scenario B, its IP is composed of trade secrets related to its various product lines. A trade secret is any confidential business information or technology that provides a company with a competitive advantage. Unlike other types of IP, trade secrets are protected indefinitely until publicly disclosed. Similar to the value of a trade name, the value of IP is estimated by approximating how much another party would pay to license that IP. To value the loss of the technology company's IP, Deloitte used the with-and-without method to compare the results of a relief-from-royalty analysis prior to the cyber incident to the results after the cyber incident. Using the method described above, Deloitte calculated the royalty rate applicable for this company at 2.5 percent. The value of the IP at the time of the cyber incident (using present-value calculations) was then derived by calculating 2.5 percent of the company's future revenues (tax-adjusted) over time. Given the characteristics of the stolen IP, its useful life was assumed to be five years and, according to assumptions provided in the company's profile, was directly tied to 50 percent of the technology company's total revenues.

Authors

Emily Mossburg
Principal | Deloitte Advisory
Cyber Risk Services
Deloitte & Touche LLP

John Gelinne
Managing Director | Deloitte Advisory
Cyber Risk Services
Deloitte & Touche LLP

Hector Calzada
Managing Director | Deloitte Advisory
Valuation Services
Deloitte Transactions and Business Analytics LLP

Contributors

Amy Kroll, Principal, Advisory Heath Care Leader, Deloitte & Touche LLP
Irfan Saif, Principal, Advisory Technology Sector Leader, Deloitte & Touche LLP
Harsh Dalwadi, Senior Manager, Cyber Risk Services, Deloitte & Touche LLP
Amy Edwards, Senior Manager, Forensic and Investigation Services, Deloitte Financial Advisory Services LLP
Emily Johns, Manager, Valuation Services, Deloitte Transactions and Business Analytics LLP
Arun Perinkolam, Senior Manager, Cyber Risk Services, Deloitte & Touche LLP
Sarah Robinson, Consultant, Cyber Risk Services, Deloitte & Touche LLP
Beth Ruck, Senior Manager, Advisory Marketing, Deloitte Services LLP

Contact us

For an electronic version of this paper, please go to:
http://www2.deloitte.com/us/beneath-the-surface-of-a-cyberattack
Please direct inquiries to cyberriskinfo@deloitte.com

Secure.Vigilant.Resilient.
To grow, streamline, and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what's most important to your organization, you must invest in cost-justified security controls to protect your most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A *Secure.Vigilant.Resilient.* cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

BEING SECURE means having risk-focused defenses around what matters most to your mission.

BEING VIGILANT means having threat awareness to know when a compromise has occurred or may be imminent.

BEING RESILIENT means having the ability to regain ground when an incident does occur.

This document contains general information only and Deloitte Advisory is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Advisory shall not be responsible for any loss sustained by any person who relies on this document.

About Deloitte
As used in this document, "Deloitte" means Deloitte & Touche LLP, Deloitte Financial Advisory Services LLP, and its affiliate, Deloitte Transactions and Business Analytics LLP. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see "http://www.deloitte.com/us/about" 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.

Copyright © 2016 Deloitte Development LLC. All rights reserved.