Global Cyber Executive Briefing

Lessons from the front lines

Deloitte.

Read more

Deloitte.

Global Cyber Executive Briefing

Lessons from the front lines

In a world increasingly driven by digital technologies and information, cyber-threat management is more than just a strategic imperative. It's a fundamental part of doing business. Yet for many C-suite executives and board members, the concept of cybersecurity remains vague and complex. Although it might be on your strategic agenda, what does it really mean? And what can your organization do to shore up its defenses and protect itself from cyber-threats?

Read more

Conclusion

This report focused on seven key industry sectors that are prime targets for cyber-attacks. Follow-on reports will highlight the top cyber-threats in other major sectors that are also highly vulnerable. After all, the single biggest takeaway from the stories and insights presented here is that breaches are inevitable -- and that no industry or organization is immune. Your organization will be hacked someday.

Read more

Sectors

High Technology
The high-tech sector is often ground zero for cyber-attacks...
Read more

Insurance
Cyber-attacks in the insurance sector are growing...
Read more

Online Media
The online media sector might have the greatest exposure...
Read more

Manufacturing
Manufacturers are increasingly being targeted not just by...
Read more

Telecom-munications
Telecom companies are a big target for cyber-attacks...
Read more

Retail
Credit card data is the new currency for hackers and...
Read more

E-Commerce & Online payments
As more and more businesses...
Read more

Lessons from the front lines

In a world increasingly driven by digital technologies and information, cyber-threat management is more than just a strategic imperative. It's a fundamental part of doing business. Yet for many C-suite executives and board members, the concept of cybersecurity remains vague and complex. Although it might be on your strategic agenda, what does it really mean? And what can your organization do to shore up its defenses and protect itself from cyber-threats?

A common myth is that cyber-attacks only happen to certain types of organizations, such as high-profile technology businesses. However, the cold, hard truth is that every organization has valuable data to lose. In fact, the attacks that happen most frequently are completely indiscriminate – using scripted, automated tools that identify and exploit whatever weaknesses they happen to find.

Cyber-attacks can be extremely harmful. Tangible costs range from stolen funds and damaged systems to regulatory fines, legal damages, and financial compensation for injured parties. However, what might hurt even more are the intangible costs -- such as loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, loss of integrity due to compromised digital assets, and overall damage to an organization's reputation and brand -- all of which can send an organization's share price plummeting, and in extreme cases can even drive a company out of business.

Being resilient to cyber-risks starts with awareness at the board and C-suite level; a recognition that at some point your organization will be attacked. You need to understand the biggest threats, and which assets are at greatest risk -- the assets at the heart of your organization's mission.

Who could potentially target your organization, and for what reasons? Which assets are attackers likely to view as most valuable? What are the possible scenarios for attack (see Table 1), and what is the potential impact to your business?

Questions such as these can help determine how advanced and persistent the cyber-threats to your business are likely to be. This insight allows you, as a C-suite executive or board member, to determine your organization's risk appetite and provide guidance that helps internal and external security professionals reduce your risk exposure to an acceptable level through a well-balanced cyber-defense. Although it isn't possible for any organization to be 100 percent secure, it is entirely possible to use a mix of processes for prevention, detection, and response to keep cyber-risk below a level set by the board and enable an organization to operate with less disruption.

Incident classification pattern	Percentage
Point of Sale System Intrusions	14%
Web App Attacks	35%
Insider Misuse	8%
Physical Theft/Loss	<1%
Miscellaneous Errors	2%
Crimeware	4%
Card Skimmers	9%
Denial of Service Attacks	<1%
Cyber-espionage	22%
Everything else	6%

Table 1: Frequency of incident classification patterns from 1367 breaches during 2013. Source: Verizon 2014 Data Breach Investigations Report [1]

[1] *http://www.verizonenterprise.com/DBIR/2014/*

Next page

To be effective and well balanced, a cyber-defense must have three key characteristics: *secure, vigilant,* and *resilient.*

Secure: Being secure means focusing protection around the risk-sensitive assets at the heart of your organization's mission — the ones that both you and your adversaries are likely to agree are the most valuable.

Vigilant: Being vigilant means establishing threat awareness throughout the organization, and developing the capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets.

Resilient: Being resilient means having the capacity to rapidly contain the damage, and mobilize the diverse resources needed to minimize impact — including direct costs and business disruption, as well as reputation and brand damage.

This executive briefing is a starting point for organizations to understand their most important cyber-threats. It highlights the top threats for seven key industry sectors -- retail, manufacturing, e-commerce & online payments, online media, high technology, telecommunications, and insurance – and offers real-world stories and practical insights to help your organization begin to assess its threat profile and stay a step ahead of cyber-criminals.

By highlighting real-life cases, we hope to make clear that being hacked is nothing to be ashamed of. Breaches occur at all organizations – not because they are badly managed, but because hackers and cyber-criminals are getting smarter every day. By sharing information about breaches we can learn how to better protect ourselves – an imperative being promoted by the *Partnering for Cyber-Resilience*[2] initiative of the World Economic Forum.

The stories clearly show that breaches are inevitable: your organization will be hacked someday. They also show that we all depend on each other for a resilient cyber-space. For example, online media can be used to spread malware; vulnerabilities in the high-tech sector affect other industries that use digital technology; and disruption in online payments impact e-commerce. By sharing and understanding these cases and taking responsibility at the C-suite and board level, we can all work together towards a safer cyber-space.

To sector

[2] *http://www.weforum.org/issues/partnering-cyber-resilience-pcr*

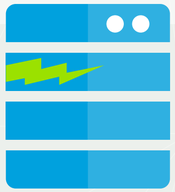
Cyber-Threats

High Technology

Cases

Fraudulent certificates lead to bankruptcy and a national security breach

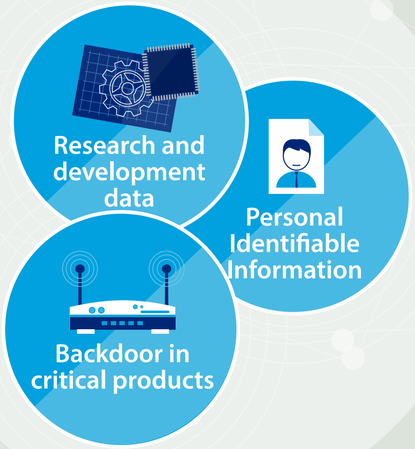
Leading software company **loses face – along with customer data** and source code



Vengeful hacktivists force a leading **online platform to shut down** for more than a month

Who?

What?



Business Impact

- **Loss of intellectual property and customer information**
- **Reduce a company's competitive advantage**
- **Great financial losses**
- **Reputation damage**

Next page

High Technology

The high-tech sector is often ground zero for cyber-attacks. One obvious reason is that these organizations have very valuable information to be stolen. However, another more subtle reason is the nature of high-tech organizations themselves. High-tech companies – and their employees – generally have a higher risk appetite than their counterparts in other sectors. Also, they tend to be early adopters of new technologies that are still maturing and are therefore especially vulnerable to attacks and exploits. For example, employees in high-tech are more likely to use (and self-administer) cutting-edge mobile devices and the latest mobile apps, which might not be secure. In addition, many high-tech organizations have open environments and corporate cultures that are designed to stimulate creativity and collaboration, but are more difficult to defend. As a result, high-tech organizations typically have a very large attack surface to protect.

Just as important, some parts of the high-tech sector provide an attack path into other sectors, since high-tech products are a key infrastructure component for all kinds of organizations. Technology is a key enabler, but it can also be a key source of vulnerability. For example, because of the tremendous need to establish trust on the internet, attacks on certificate authorities have caused serious privacy breaches across a number of industries. Also, vulnerabilities in point-of-sale systems have led to major security breaches for retailers, and back doors in communication hardware have exposed organizations in every sector to a wide range of attacks.

Speaking of back doors, the growing involvement of covert state actors in this area has been making headlines recently, causing serious reputational damage for the organizations involved.

For companies in the high-tech sector, one of the biggest threats is loss of intellectual property (IP). Having IP lost or stolen after years of investment can dramatically reduce an organization's competitive advantage (which involved both IP and personal information). States and competitors are often the actors in IP theft; however, insiders are also a major threat. A single highly skilled insider with the right kind of access can quickly make off with huge amounts of valuable data.

Since many high-tech companies also offer online services, loss of customer information is another major threat that is highly visible, since many countries require disclosure when personal identifiable information is lost. However, IP theft might actually be more prevalent. It's hard to know for sure based on media coverage since there is generally no requirement to disclose lost IP.

Hacktivism is another significant threat in this sector. High-tech companies create products that technically savvy people are keen to "hack" in the original sense of the word, which means using something for a purpose other than what it was designed for. Organizations that prosecute or sue people for this type of "hacking" may find themselves targeted by hacktivist groups, which can lead to great financial losses and reputation damage.

Case 1

Fraudulent certificates lead to bankruptcy and a national security breach

Case 2

Leading software company loses face – along with customer data and source code

Case 3

Vengeful hacktivists force a leading online platform to shut down for more than a month

High Technology

Case 1

Fraudulent certificates lead to bankruptcy and a national security breach

Organization
A certificate authority that signs security certificates for organizations globally.

Scenario
The internet is based on trust and certificate authorities are at the heart of this trust. Hackers with ties to a foreign government obtained illegal access to the certificate authority's servers and used it to generate fraudulent security certificates. These certificates were then used to enable fraudulent servers posing as the original servers belonging to highly used web services. This allowed the attackers to perform man-in-the-middle attacks, possibly intercepting and decrypting a tremendous amount of confidential communications.

Attackers and motivation
The individual who claimed the attack said he was driven by political beliefs. However, the way the fraudulent certificates were used and the fact that the attack took place over a relatively long period of time suggests state actors were also involved.

Techniques used
Apart from known hacker tools, some very complex attack scripts were used that were specifically developed to attack the certificate authority in question.

Business impact
The hackers generated more than 500 fraudulent certificates, which were then used to perform man-in-the-middle attacks against many well-known global services. The certificate authority could not guarantee revocation of the fraudulent certificates, which was completely unacceptable given that the organization's sole reason for existence is to provide certification that is 100% trustworthy. The certificate authority declared bankruptcy shortly after the breach was made public.

High Technology

Case 2

Leading software company loses face – along with customer data and source code

Organization
A large software vendor that sells software globally, with more than $1 billion in annual revenue.

Scenario
Hackers infiltrated the company's network and downloaded more than 100 million encrypted user credentials, along with credit card information for millions of customers. In addition, the source code for a number of key products was stolen.

Attackers and motivation
No one has claimed the attack and information about the attackers is not publicly known. However, given the type of information stolen, it is likely this was the work of an organized group of cyber-criminals aiming to use the stolen credentials for identity theft, and to sell the stolen source code for financial gain. Also, since the stolen source code was for a widely used application, it's possible that the application itself will be used as an attack vector, since finding vulnerabilities is much easier with the source code in hand.

Techniques used
The company's Chief Security Officer described the attack as "sophisticated". Other than that, no details have been made public.

Business impact
This story made global headlines, dealing a severe blow to the company's reputation -- especially since people expect better security practices from a software vendor. The company had to require more than 100 million users to change their passwords, and offered a large portion of their customers a year of free credit monitoring. In addition, the loss of its source code could significantly reduce the company's long-term competitive advantage.

High Technology

Case 3

Vengeful hacktivists force a leading online platform to shut down for more than a month

Organization
A very large technology company that sells products all around the world and operates a popular online platform.

Scenario
The online platform, which has millions of users, was attacked by a hacktivist group with a grudge against the company. The hackers managed to steal more than 70 million user names and passwords, as well as credit card information in multiple attacks spanning months. In the wake of the attack, the company was forced to temporarily shut down its online service, denying access to users for more than a month.

Attackers and motivation
Prior to the attack, the company had made some decisions in a public case that did not sit well with a particular group of clever hackers. This hacktivist group sought revenge by hitting the company with a very impactful attack.

Techniques used
The initial attack vector the hackers used to infiltrate the company's network is not publicly known. What is known however is that the attackers spent a long time in the company's internal network. During this time they discovered a number of vulnerabilities that could be easily exploited. Most likely they used a SQL injection attack against the online platform's internet-facing servers to steal data from sensitive databases.

Business impact
The company lost personal and credit card information for more than 70 million users.
Also, because the attackers were so deeply nested in the internal network, the company decided to close down the online platform for multiple months resulting in major financial losses. Customers were later compensated for the downtime, costing the company even more money. What's more, the breach was reported in the news globally, badly damaging the organization's reputation.

Cyber-Threats

Online media

Cases

Email addresses stolen from an email service provider

News website is the launch pad for a **banking malware outbreak**

Readers redirected to **fake news**

Who?

What?

Business Impact

- **Reputational damage**
- **Spread propaganda**
- **Manipulate public opinion**

Next page

Online Media

Previous page

The online media sector might have the greatest exposure to cyber-threats. Since its organizations operate online, they have a huge attack surface to protect. Also, since its products are in high demand and completely digital, there is a high risk of being infiltrated and robbed of valuable content – both by individuals and organized crime groups.

As in other industries, attacks that use an organization's website as the point of entry are common. So are social engineering attacks, such as spear phishing, which trick people into giving away passwords and other sensitive information. However, what makes the online media industry unique is the fact that the sector itself can serve as a vector for launching attacks, due to the large number of people who use its services. A good example of this is the "watering hole" attack, in which hackers breach a popular website and then use it as a delivery platform for malware.

Another threat that uses online media itself as the attack vector involves manipulating news sources to trick people or automated programs into making misinformed decisions. There are many well known examples of high profile online media accounts being hacked and fed deceptive information. In one extreme case, the attack triggered a stock market crash by fooling stock trading programs into placing automatic sell orders based on false information from a political online media account.

For online media organizations, attacks that cause reputational damage are one of the biggest threats. News organizations in particular are increasingly popular targets for hacktivists and attack groups loyal to a particular nation or cause. Some of these attacks target specific reporters in an effort to uncover their sources; other attacks disrupt websites or present substitute content in order to damage an organization's reputation, spread propaganda, or manipulate public opinion.

Case 1

Email addresses stolen from an email service provider

Case 2

News website is the launch pad for a banking malware outbreak

Case 3

Hackers redirect readers to fake news

Online Media

Case 1

Email addresses stolen from an email service provider

Organization
A company that provides email services for more than 2,000 large organizations in all sectors, sending billions of marketing and customer communications emails annually.

Scenario
An unknown group of hackers breached the company's databases and stole nearly 60 million email addresses.

Attackers and motivation
Little is publicly known about the attackers. They might have been "script kiddies" hacking for fun, organized criminals planning to use the email addresses for spear phishing attacks, or perhaps a competitor trying to embarrass the company.

Techniques used
Although the exact technique has not been disclosed, experts believe it was something simple, such as SQL injection. This might explain why the company has been reluctant to share details about the attack.

Business impact
Although this breach only involved names and email addresses, not financial information, it was very damaging because it was directly related to the company's core business of sending marketing emails on behalf of clients. Also, the sheer size of the data loss drew a lot of attention from the media. The company was forced to notify all affected clients, who in turn had to notify their own customers, since this massive leakage of email addresses exposed them to spear phishing attacks. This made both the company and its clients look bad. In tangible terms, this breach cost the company and its clients an estimated $200 million in customer compensation.

Online Media

Case 2

News website is the launch pad for a banking malware outbreak

Organization
A company hosting a news website that ranks in the top 20 of most visited websites within the country it serves.

Scenario
Attackers used the website as a platform to spread malware. They established this by gaining access to a third-party advertisement system, which they then used to place infected advertisements on the news website. When clicked, the infected ads checked the user's software version, and when a vulnerable version was found installed malware on the victim's computer that would hijack banking transactions and steal card payment information.

Attackers and motivation
The complexity of the attacks and use of banking malware strongly suggest an organized crime group out for financial gain.

Techniques used
This attack used malware specifically designed to steal money from online banking users in the country where the website is hosted. How the attackers obtained the credentials to the third-party systems that distribute advertisements is not known, but once they gained access, it's clear they used infected advertorials to spread the malware.

Business impact
As the launch pad for a large outbreak of banking malware, the organization's reputation took a big hit. Also, since the organization makes almost all of its money from online media, its number one priority and challenge was to restore readers' and advertisers' trust in online advertisements.

Online Media

Case 3

Hackers redirect readers to fake news

Organization
A large news organization, with a strong presence both online (websites) and offline (newspapers).

Scenario
A hacker group with political ties tricked employees of a third-party domain registrar into revealing information that was then used to access domain name server (DNS) records, allowing the group to redirect all incoming web traffic to its own website.

Attackers and motivation
The attackers were hacktivists spreading propaganda and wanting to influence public opinion about events occurring in their region.

Techniques used
The attackers used social engineering, in particular spear phishing, to gain access to the reseller's DNS account. It then altered DNS records to redirect web traffic to its own server, which hosted a visually identical copy of the news website but presented altered facts.

Business impact
The attack tarnished the organization's reputation and credibility, which because of the organization's size and name recognition, also had a ripple effect on other news organizations. This caused readers to question the legitimacy of news stories they viewed online, and likely drove some to other news sources.

Cyber-Threats

Telecommunications

Cases

State-sponsored hackers launch **privacy attack**

False claims do real damage to a major ISP

Thief steals a laptop containing personal information of customers

Who?

What?

Business Impact

- **Damage company's reputations**
- **Underminded customer trust**
- **Loss of confidental information of organization**

Next page

Telecommunications

Telecom companies are a big target for cyber-attacks because they build, control and operate critical infrastructure that is widely used to communicate and store large amounts of sensitive data.

Government agencies are increasingly attacking telecom operators' infrastructure and applications to establish covert surveillance. These sophisticated actors typically use very advanced persistent threats (APT) that can operate undetected for long periods of time. Communication channels targeted for covert surveillance include everything from phone lines and online chat to mobile phone data. There have even been cases where one nation's cyber-attack prevented another nation's leaders from communicating on their mobile devices.

Given that telecom companies control critical infrastructure, the impact of an attack can be very high and far-reaching. In fact, even the false claim of an attack can force a telecom company to shut down critical services that consumers and businesses rely on.

Customer data is another popular high impact target. Telecom organizations typically store personal information -- such as names, addresses and financial data – about all of their customers. This sensitive data is a compelling target for cyber-criminals or insiders looking to blackmail customers, conduct identity theft, steal money or launch further attacks. Information can be lost in a variety of ways that may be as simple as a stolen laptop. Of course, laptops can be lost or stolen in any sector; however, the problem tends to be worse in telecom because employees in this sector often serve customers as part of a call center or help desk function and may have large amounts of sensitive customer data stored on their laptops.

One critical threat unique to the telecommunications sector is the attack of leased infrastructure equipment, such as home routers from Internet Service Providers (ISPs). Once the equipment has been compromised, hackers can use it to steal data, launch other attacks anonymously, store exfiltrated data, or access expensive services such as international phone calls. To avoid upsetting customers, telecom companies generally refund any charges associated with such attacks, often resulting in significant lost revenue.

Case 1

State-sponsored hackers launch privacy attack

Case 2

False claims do real damage to a major ISP

Case 3

Thief steals a laptop containing sensitive customer information

Telecommunications

Case 1

State-sponsored hackers launch privacy attack

Organization
A very large international mobile phone provider.

Scenario
Cyber spies gained access to mobile communication channels for surveillance purposes by incorporating malicious software on a spoofed social media page of privileged users within the company.

Attackers and motivation
The attackers were associated with a government agency that wanted to spy on large groups of mobile phone users.

Techniques used
The attack was an extremely sophisticated combination of several techniques. The attackers first spoofed the personal social media pages of privileged users within the company. The spoofed pages then installed malicious software on the users' computers, taking advantage of their elevated system privileges to penetrate deeply into the company's network. This ultimately allowed the attackers to access mobile communication data for surveillance purposes.

Business impact
The size and scope of the attack did significant damage to the organization's reputation and confidentiality of the infrastructure. It also fueled customer concerns about privacy, which is a major issue for the entire telecom sector.

Telecommunications

Case 2

False claims do real damage to a major ISP

Organization
A large internet service provider (ISP), hosting a nation's critical infrastructure.

Scenario
A teenage hacker gained access to hundreds of the ISP's servers and then published a list of user names and passwords he claimed to have stolen from them. This forced the company to temporarily suspend the email accounts of all affected users. It later turned out the data was obtained from a different company and not the ISP.

Attackers and motivation
The attacker was an individual teenager who was hacking for fun and ego gratification, bragging about his accomplishments in online forums.

Techniques used
A vulnerability in a website not related to the affected company was exploited to export data from the database containing customer information. The attacker then selected all users having email addresses from the ISP's domain in order to make the public (and the ISP itself) believe the ISP had been compromised.

Business impact
The ISP did not have the proper processes in place to determine if it had been compromised or not, and thus had to assume the published data had been stolen from its systems. In response, it was forced to suspend all affected email accounts, which angered a lot of customers and prompted many to switch to another email provider. Also, the fact that the ISP could not conclusively determine if the leaked data had actually originated from its systems gave the impression the company did not have a very good handle on security breaches.

Back to sector

Next case

Telecommunications

Case 3

Thief steals a laptop containing sensitive customer information

Organization
A very large cable service provider that offers television, internet and mobile telephony services.

Scenario
One of the organization's employees – in violation of company policy -- had stored a lot of sensitive customer information on his laptop. The laptop was an older model and the data was stored unencrypted. Personal information for 40,000 customers was lost, including client numbers, names, email-addresses, postal codes, genders and parts of bank account numbers.

Attackers and motivation
The attacker was a petty thief who was interested in the laptop, not the data. In fact, it's likely he didn't even know the data was there.

Techniques used
Although the technique of stealing a physical laptop was not sophisticated or specifically relevant for the Telecommunications sector, the type of data that resided on it was.

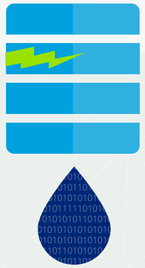
Business impact
It's unclear whether the stolen data was used maliciously since the thief may not have even realized it was there. However, all affected customers had to be informed of the incident, leading to loss of trust. Also, extensive media coverage caused significant embarrassment and reputation damage for the company.

Cyber-Threats

E-Commerce & Online payments

Cases

Lost customer data leads to lost trust

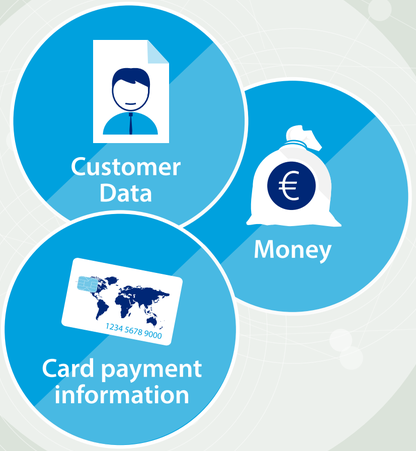


Hacktivists strike back with a vengeance

Thieves use stolen data to **create their own credit cards**

Who?

What?



Business Impact

- **Loss of trust, money and services**
- **Identity theft of customers**
- **Non-Compliance issues**

Next page

E-Commerce & Online payments

Previous page

As more and more businesses move or expand from bricks to clicks, criminals are following suit. Many e-commerce websites are directly connected both to the internet and to a company's back-end systems for data processing and supply management, making the website a prime attack point for gaining access to crucial information assets within the organization.

One of the most common attacks in this sector is a database breach. Often, such attacks result in a loss of customer data, including names, physical addresses, phone numbers, e-mail addresses and payment information. Since trust is especially important in e-commerce, the loss of customer data can be very damaging to an online company's reputation and business performance. This is true even if the attacker is an unsophisticated "script kiddie" who is just showing off for friends or messing around for fun. Also, the impact of a breach can go far beyond reputation damage, depending on where in the world it occurred. A number of US states have already instituted breach notification laws, and the EU is expected to follow shortly. Such laws require organizations to come forward and publically admit they were breached. The EU directive also includes heavy fines.

Online payment systems are another vulnerable area that is often attacked. The ability to accept payment is critically important for online businesses, since it is one of the last steps in a customer's purchase journey. As such, the financial impact of a payment system attack can be enormous, depending on its duration. After all, if customers can't pay, they can't buy.

Most e-commerce sites outsource payment processing to a variety of third-party providers that promise high availability of their payment services. However, these providers are increasingly being targeted with denial-of-service attacks, particularly by hacktivists that want to disrupt an organization in a highly visible way.

Payment-related attacks are also appealing to criminals looking for financial gain. Saving a customer's credit card data in an internal database might seem like a good way to make the shopping process more convenient, but it creates an attractive target for cyber-criminals. Payment processing vendors are even more attractive to attack, since the potential for a big score is much greater. In the brick-and-mortar world, cyber-criminals have developed a variety of techniques for skimming credit cards at Point of Sale (POS) terminals and ATMs. Also, they have developed a wide range of attack vectors targeted directly at online payment vendors. Some of the most sophisticated attacks use a combination of online and traditional physical techniques to increase their effectiveness.

Attacks on a payment vendor can be just as damaging to a company's reputation as attacks that target the business directly, since most customers don't see a distinction between an organization and its service providers.

Case 1

Lost customer data leads to lost trust

Case 2

Hacktivists strike back with a vengeance

Case 3

Thieves use stolen data to create their own credit cards

E-Commerce & Online payments

Case 1

Lost customer data leads to lost trust

Organization
An e-commerce company that operates daily deals websites in numerous countries.

Scenario
Hackers breached the security of the organization's computer system, resulting in unauthorized access to customer data.

Attackers and motivation
The attackers were most likely after customer credit card data to sell on the black market.

Techniques used
SQL Injection, which is the most common form of attack for websites and web applications, was most likely used for this breach. However, other entry methods cannot be ruled out, including a more sophisticated cross-site scripting attack, or perhaps exploitation of a flaw in the web application that might have resulted from poor testing.

Business impact
More than 50 million usernames, hashed passwords and e-mail addresses were stolen, badly damaging the company's reputation. And because customer data was involved, the organization was required to report the breach, which attracted attention from the media. The incident received worldwide press coverage, both in newspapers and on television. What's more, loss of personal data resulted in a loss of customer trust, which is especially critical for e-commerce companies. This almost certainly had a negative impact on revenue.

E-Commerce & Online payments

Case 2

Hacktivists strike back with a vengeance

Organization
A very large financial services firm whose core global business is processing credit card transactions.

Scenario
A popular protest turned into cyber-terrorism with a call–to-action from a politically motivated hacker collective. Together, thousands of people initiated a large denial-of-service attack on the company's network, making its services unavailable to clients.

Attackers and motivation
The attack was motivated by the company's decision to block payments to a well known website based on claims that the site's activities were illegal. This decision caused a worldwide commotion among the website's supporters. Popular support for the cause -- combined with low technical requirements to participate -- resulted in a large-scale attack.

Techniques used
To make the attack as successful as it was, the hackers recruited a large numbers of volunteers to help. All participants installed special attack software on their computers, which together formed a single large botnet. The software was specifically designed to perform a large distributed denial-of-service attack (DDoS) on the company's network. Instructions were sent via chat telling all of the computers in the botnet to start attacking the company's network. Due to the large number of people involved in the attack, the company's payment services quickly became unavailable or highly inaccessible for 10 hours.

Business impact
Direct costs of the attack have been estimated at more than $3 million. But the incident's overall impact was even greater, showing how cyber-protests could be used to damage organizations and influence their behavior. Since the attack, other organizations within the sector have been targeted for protest by the same group.

E-Commerce & Online payments

Case 3

Thieves use stolen data to create their own credit cards

Organization
A large financial services firms that provides electronic transaction processing worldwide.

Scenario
A group of criminals broke into the company's systems and over the course of a year stole magnetic stripe data for approximately 7 million credit cards. They then created fake credit cards by programming the stolen data onto cheap prepaid cards, which were later used to purchase expensive items such as computers and televisions.

Attackers and motivation
The attackers were motivated by financial gain. The careful target selection and sophisticated techniques used for the attack suggest the involvement of a well organized cyber-criminal group.

Techniques used
Attackers infiltrated a crucial part of the payment processing infrastructure containing magnetic stripe data, which was then exported to create duplicate credit cards that were later used for fraudulent transactions.

Business impact
The company revealed that the data breach cost an estimated $90 million, which includes fraud losses as well as fines, costs associated with the investigation, charges from card networks and client aftercare. The company's reputation also took a lot of damage, both from consumers and from clients within the payment card networks.

Cyber-Threats

Insurance

Cases

Hackers steal personal data about customers - and potential customers

Even small **breaches can have a meaningful impact** and require corrective action

Targeted insurer accused of **doing too little too late**

Who?

What?

Business Impact

Tangible costs related to legal fees, fines, lawsuits, fraud monitoring costs

Intangible costs such as customers' trust

Customer compensation

Next page

Insurance

Cyber-attacks in the insurance sector are growing exponentially as insurance companies migrate toward digital channels in an effort to create tighter customer relationships, offer new products and expand their share of customers' financial portfolios. This shift is driving increased investment in traditional core IT systems (e.g., policy and claims systems) as well as in highly integrated enabling platforms such as agency portals, online policy applications and web- and mobile-based apps for filing claims. Although these digital investments provide new strategic capabilities, they also introduce new cyber-risks and attack vectors to organizations that are relatively inexperienced at dealing with the challenges of an omni-channel environment. What's more, the challenges are likely to become more complex as insurers embrace big data and advanced analytics that require collecting and handling vast amounts of consumer information. As insurers find new and innovative ways to analyze data, they must also find ways to secure the data from cyber-attacks.

Cyber-criminals have started to recognize that insurers possess large amounts of personal information about their customers, which is very attractive to identity thieves and fraudsters. In some cases, insurers also possess significant amounts of customer credit card and payment data. However, there is at least one case in the insurance sector where the victims of a cyber-attack weren't even paying customers but merely consumers who had requested a price quote.

Cyber-criminals targeting insurers often have significant resources. This enables them to employ sophisticated attacks that combine advanced malware with other techniques such as social engineering.

Attacks on insurance firms can result in significant, tangible damages such as fines, legal fees, lawsuits and fraud monitoring costs. However, a less obvious but no less significant impact may be loss of trust, driven by customers' concerns about whether their information is truly safe. Since the insurance business revolves around trust, a major breach can have a very real impact on an insurer's brand and market value.

It's worth noting that most of the breaches publicly reported by insurance companies to date have been characterized as short-term attacks, with cyber-criminals compromising a system, stealing specific information and then quickly moving on. In fact, our research did not uncover any documented cases of long-term infiltration and cyber-crime in the insurance sector. However, we believe the number of long-term attacks may be silently growing as attackers quietly slip in undetected and establish a persistent, ongoing presence in critical IT environments.

Over the years, many insurance organizations have invested a lot of money in security tools and processes that may be providing a false sense of security. As attackers learn to leverage encryption and other advanced attack techniques, traditional tools such as firewalls, antivirus software, intrusion detection systems (IDS) and intrusion preven¬tion systems (IPS) are becoming less and less effective. As a result, many insurers may be misallocating their limited resources to address compliance-oriented, easily recognized threats while completely overlooking stealthy long-term threats that ultimately could be far more damaging.

Case 1

Hackers steal personal data about customers -- and potential customers

Case 2

Even small breaches can have a meaningful impact and require corrective action

Case 3

Targeted insurer accused of doing too little too late

Insurance

Case 1

Hackers steal personal data about customers -- and potential customers

Organization
A group of large insurance and financial services companies.

Scenario
Cyber-criminals breached the company database and stole information of more than one million customers and sales prospects, including driver's license data and social security numbers.

Attackers and motivation
Cyber-criminals were after personal identifiable information in order to sell it on the black market for identity fraud purposes.

Techniques used
Part of the network used by the organization's members was breached by cyber-criminals and used to steal customer information.

Business impact
The organization was obliged to provide affected customers with free credit monitoring for a year, and to reimburse all damages resulting from the breach. In addition to those tangible costs – which were substantial -- the organization suffered significant brand damage and loss of trust.

Insurance

Case 2

Even small breaches can have a meaningful impact and require corrective action

Organization
A very large investment and insurance company.

Scenario
The attack targeted company employees with e-mails containing malware that could capture confidential data such as bank account numbers, social security numbers, user accounts/logins, passwords and credit card numbers. Hackers used this information to compromise several servers, including servers used by employees to remotely access the company's IT systems.

Attackers and motivation
Cyber-criminals were after online banking information to perpetrate fraud for financial gain.

Techniques used
The attack targeted company employees with e-mails containing malicious software that could capture confidential data such as bank account numbers, social security numbers, user accounts/logins, passwords and credit card numbers.

Business impact
Although the attack affected only a small number of employees -- and only a handful of customers -- it still received media coverage that damaged the company's reputation.

Insurance

Case 3

Targeted insurer accused of doing too little too late

Organization
An insurance and financial services firm that specializes in serving seniors.

Scenario
Attackers exploited vulnerable software on the company's servers and stole payment card information for more than 93,000 customers, including names, addresses and unencrypted card security codes.

Attackers and motivation
Cyber-criminals were after payment card information to sell on the black market and commit fraudulent transactions.

Techniques used
Vulnerabilities in the company's systems and software were discovered and exploited by the cyber-criminals to gain access to payment card information.

Business impact
The company immediately removed the vulnerable IT elements and had to issue a formal apology. It also offered free identify fraud monitoring to affected customers. However, the company has been strongly criticized for retaining unencrypted security codes --which is a noncompliance issue according to the Payment Card Industry Data Security Standard (PCI DSS) -- and for not reporting the breach to its customers sooner.

Cyber-Threats

Manufacturing

Cases

Malware snares employee log-in credentials

Worm grabs control of industrial plants

Executive pilfers intellectual property from a competitor

Who?

- Hacktivists
- State Actors
- Competitors

What?

- Market Advantage
- Intellectual Property
- Industrial Control Systems

Business Impact

Reputational damage

Loss of a competitive advantage and production

Next page

Manufacturing

Manufacturers are increasingly being targeted not just by traditional malicious actors such as hackers and cyber-criminals, but by competing companies and nations engaged in corporate espionage. Motivations range from money and revenge to competitive advantage and strategic disruption.

What happens to a manufacturing business when its production operations suddenly grind to a halt? And what are the consequences of being unable to satisfy market demand? In today's business environment of increased automation, connectivity and globalization, even the most powerful organizations in the world are vulnerable to debilitating cyber-threats. Also, as production spreads across the globe, regional and national politics are becoming an increasingly important factor in corporate and manufacturing policies.

Many existing manufacturing systems were developed at a time when security was much less of an issue. Also, the focus of manufacturing technology has traditionally been on performance and safety, not security. This has led to major security gaps in production systems. In addition, the growing complexity of these systems has resulted in large and elaborate network infrastructures that are extremely specialized. And in many cases the systems are being operated and managed by manufacturing specialists rather than the IT function. Combined with the integration of IT and operations, these trends have created a system environment with a large attack surface that is very difficult to manage and secure.

Types of cyber-attacks in manufacturing vary widely. Traditional attacks involve hackers gaining unauthorized access to sensitive systems and data. Phishing facilitates the process by tricking executives and their staffs into revealing login credentials and other private information, giving attackers front-door access to the organization's systems.

Advanced malware is another type of attack that is increasingly common in manufacturing – and increasingly disruptive. In an era of ubiquitous connectivity when more and more industrial systems are connected to the internet, this malicious software infiltrates weak systems and hardware (often legacy manufacturing systems) and then spreads itself to other systems, leaving behind a trail of destruction and disruption.

Internal threats, although often less technically sophisticated, can be just as damaging. In manufacturing, there are countless incidents of malicious insiders stealing a company's intellectual property or other confidential information for personal profit or revenge. These internal attacks can be committed by current and former employees and contractors at any level of the organization – even the executive level.

The results of any of these attacks can be severe, ranging from loss of valuable ideas and market advantage to financial and reputational damage -- particularly in cases where sensitive customer data is compromised.

Case 1

Malware snares employee log-in credentials

Case 2

Worm grabs control of industrial plants

Case 3

Executive pilfers intellectual property from a competitor

Manufacturing

Case 1

Malware snares employee log-in credentials

Organization
A large, global automotive manufacturer.

Scenario
Attackers infiltrated the manufacturer's corporate network and installed malicious software. This malware allowed the attackers to obtain employee log-in credentials, which in turn could be used to target other key systems within the company that contained intellectual property.

Attackers and motivation
The attack targeted intellectual property related to automotive technology. This type of IP is very valuable and can be used to blackmail the company, or to gain competitive advantage. A close analysis of the incident suggests the attackers were part of an organized crime group.

Techniques used
The attackers used a mix of techniques to deploy the malware into the company's network, including targeted email attacks and exploiting vulnerabilities in outdated systems.

Business impact
The incident received global media coverage, causing significant reputational damage to the company. However, the potential damage was reduced by the fact that the organization fixed the security flaws before making a statement to the press. This gave the organization time to investigate the attack and to determine it had not lost any information other than the employee login credentials.

Manufacturing

Case 2

Worm grabs control of industrial plants

Organization
A multinational engineering and electronics firm with global operations.

Scenario
Attackers used a variant of advanced malware to infect multiple industrial plants around the world. Once the infection spread, the attackers could take control of systems used to monitor and control critical industrial systems such as power plants, and influence their inner workings.

Attackers and motivation
These type of attacks typically target high value infrastructure with the goal of causing widespread damage to an organization or even to an entire nation. The level of complexity, sophistication and funding needed for this attack suggests the actors were most likely state-sponsored.

Techniques used
To deploy the malware into the industrial plants, the attackers used infected removable media such as USB devices. Once an infected device was connected to a plant's internal network, the advanced malware was automatically deployed -- grabbing control of the plant and running commands to influence its supervisory control and data acquisition (SCADA) systems.

Business impact
Official statements by the company emphasized that no real damage had been done to any of the infiltrated plants. However, the incident still created a huge stir in the media and significantly damaged the company's reputation, since the attackers were theoretically able to control high value infrastructure that could have wreaked havoc on the environment.

Manufacturing

Case 3

Executive pilfers intellectual property from a competitor

Organization
A leading manufacturer of video cameras and other digital cinematography tools.

Scenario
The company had valuable intellectual property (IP) stolen by a competing executive. The company was sharing its IP via email with the executive's former employer to explore a possible joint venture, and the executive used old login credentials to gain access to the emails.

Attackers and motivation
The attacker was a rival industry executive who wanted to get an unfair advantage over his competitors by using their intellectual property to enhance his own company's products.

Techniques used
The executive obtained the login information while working at his former employer, which made the mistake of not removing or deactivating his account after he left for another firm. This allowed the executive to continue accessing his former employer's email and redirect the exchange of intellectual property to his current email account.

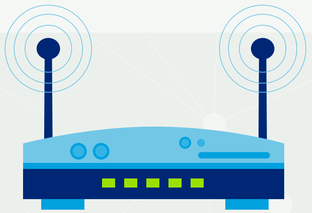
Business impact
IP theft can lead to a flood of counterfeit products. In this case, the targeted company lost a hard-earned competitive advantage derived from years of cutting-edge research and development. After the theft, its products no longer stood out in the marketplace, which weakened its sales and strategic market position.

Cyber-Threats

Retail

Cases

Weak wireless security provides an open door to attack



Inside job goes undetected for years

Hackers **steal card data** on millions of customers

Who?

- Insiders
- Cyber-criminals
- Contractors

What?

- Cardholder Data
- Personal Data
- Intellectual Property

Business Impact

- **Damage company's brand**
- **Cut into sales**
- **Fines and settlement costs**

Next page

Retail

Previous page

Credit card data is the new currency for hackers and criminals, and retailers possess a lot of it. This makes the retail industry an almost irresistible target for cyber-attacks.

The industry's attack surface is expanding as retailers of every shape and size look to boost sales and improve efficiency by harnessing the latest data-driven technologies. Use of big data and sophisticated data warehouse models is growing fast. Also, many retailers are getting into the healthcare and pharmacy businesses, and as such are holding more sensitive data than ever before. Meanwhile, there is a steady shift from cash payments to electronic card payments in developing countries.

Insider threats in retail are also rising. Employee turnover is high, and the typical retailer has many points of insider vulnerability, including seasonal and traditional employees, as well as numerous stores and distribution centers. Many retailers also outsource some of their business processes to third parties.

Trends such as these are giving rise to a new breed of criminals. Instead of stealing money or physical goods from a store or warehouse, these cyber-criminals focus on stealing information -- especially the valuable cardholder data that flows between consumers and retailers.

System access by employees and third-party contractors should be tied to job functions and carefully planned and monitored. Access to specific data fields should be carefully planned as well due to the threat of data aggregation (creating sensitive data by piecing together seemingly benign data from various data sources).

Point-of-sale (POS) systems are an increasingly popular point of attack for acquiring transaction data, giving cyber-criminals immediate access to valuable information such as card numbers and personal identification numbers (PINs).

Traditional data sources within the organization are also vulnerable. These include databases containing customer information, as well as intellectual property valuable to competitors, such as planned future store locations and demographic data (e.g., average income or age in a shop's region).

Some attacks use advanced technology that take advantage of weaknesses in the IT infrastructure. Other attacks are as simple as an insider copying data to portable media and then walking out the door.

Whether an attack is simple or sophisticated, the results can be disastrous. Retailers today must understand the potential threats and take aggressive action to protect themselves and their customers from harm.

Case 1

Hackers steal card data on millions of customers

Case 2

Weak wireless security provides an open door to attack

Case 3

Inside job goes undetected for years

Retail

Case 1

Hackers steal card data on millions of customers

Organization
A large retailer that sells a variety of food and non-food products.

Scenario
Attackers installed malware on the retailer's point-of-sale (POS) systems. The infected systems recorded the data for every card swiped through the machine, including PINs. The malware was also capable of spreading itself throughout the organization, eventually infecting millions of POS systems within the retailer and collecting vast amounts of credit card data that was later resold for illicit purposes.

Attackers and motivation
The attackers were identified as organized criminals motivated by the potential financial gain from selling huge amounts of credit card information.

Techniques used
This attack used malware that can be purchased on the criminal market. The attackers installed the malware into the retailer's environment, where it spread itself onto point-of-sale systems that could then be used to extract confidential data and create other backdoors into the retailer's network.

Business impact
The attack received worldwide media coverage, severely damaging the company's brand and cutting into sales. Financial impacts included: a drop in the company's share price over the following quarter and into the next fiscal year; heavy fines; and the cost of offering free credit monitoring to millions of customers.

Retail

Case 2

Weak wireless security provides an open door to attack

Organization
A large retailer that sells apparel and home fashions.

Scenario
Attackers were able to exploit weak security on one of the retailer's wireless networks, which allowed them to intercept card transactions and access the organization's central database. The database, which was not encrypted, contained personal information and credit card details. As a result, the attackers were able to simply download the database and start selling the stolen information through a wide variety of channels.

Attackers and motivation
The attackers were cyber-criminals motivated by the financial gain of selling personal and cardholder data.

Techniques used
Several different techniques for attacking wireless networks were used to gain access to the network. Once inside, the attackers were able to monitor and intercept network data that eventually gave them access to the database of confidential information.

Business impact
The retailer's reputation took a big hit due to the large amount of personal identifiable and credit card information that was lost. This had a significant financial impact, including fines, settlement costs and lost sales.

Retail

Case 3

Inside job goes undetected for years

Organization
A large retailer that sells communication-related products and services.

Scenario
Over the course of several years an employee of the retailer was able to obtain more than 8 million pieces of sensitive data, including personal information and classified documents. The employee sold the information to the highest bidders, which often included criminal organizations.

Attackers and motivation
The attacker was an employee who had worked at the retailer for many years. The employee was motivated by the financial gain from selling confidential information.

Techniques used
This incident illustrates that a very severe breach does not require sophisticated attack patterns. In this particular case, the attacker had direct access to confidential information and simply copied it onto portable media and took it home at the end of the day.

Business impact
The magnitude and especially the duration of the attack damaged the company's reputation and share price. Other impacts included financial compensation for customers affected by the breach, as well as lasting mistrust of employees.

Back to sector

Conclusion

Conclusion

This report focused on seven key industry sectors that are prime targets for cyber-attacks. Follow-on reports will highlight the top cyber-threats in other major sectors that are also highly vulnerable. After all, the single biggest takeaway from the stories and insights presented here is that breaches are inevitable -- and that no industry or organization is immune. Your organization will be hacked someday.

Attacks can result in significant tangible costs ranging from stolen money and property to regulatory fines, legal damages, and financial compensation. But those are just the tip of the iceberg. The really significant costs are the intangibles, particularly loss of competitive advantage, loss of customer trust, and damage to an organization's reputation and brand. Intangibles such as these can have a major impact on an organization's strategic market position and share price.

The good news is that cyber-threats are a manageable problem. As noted earlier, a well-balanced cyber-defense needs to be *secure, vigilant,* and *resilient*. Although it isn't possible for any organization to be 100 percent secure, by focusing on these three key attributes, it is entirely possible to manage and mitigate cyber-threats in a way that reduces their impact and minimizes the potential for business disruption.

In closing, here are five takeaway questions to reflect on through the lens of a *secure, vigilant,* and *resilient* approach to cybersecurity:

1. **Are we focused on the right things?**
   Often asked, but difficult to accomplish. Understand how value is created in your organization, where your critical assets are, how they are vulnerable to key threats. Practice defense-in-depth.

2. **Do we have the right talent?**
   Quality over quantity. There may not be enough talent to do everything in-house, so take a strategic approach to sourcing decisions. Are the security teams focused on the real business areas?

3. **Are we proactive or reactive?**
   Retrofitting for security is very expensive. Build it upfront in your management processes, applications, and infrastructure.

4. **Are we incentivizing openness and collaboration?**
   Build strong relationships with partners, law enforcement, regulators, and vendors. Foster internal cooperation across groups and functions, and ensure that people aren't hiding risks to protect themselves.

5. **Are we adapting to change?**
   Policy reviews, assessments, and rehearsals of crisis response processes should be regularized to establish a culture of perpetual adaptation to the threat and risk landscape.

Contact

Contact

Deloitte Cyber Leaders

Global
Kelly Bissell
KBissell@deloitte.com
+1 4042201187

EMEA
Fernando Picatoste
FPicatoste@deloitte.es
+34 915145000

APAC
Victor Keong
VKeong@deloitte.com
+65 62248288

LATCO
Martin Carmuega
MCarmuega@deloitte.com
+54 1143202700

Americas
Edward Powers
EPowers@deloitte.com
+1 2124365599

Nick Galletto
NGalletto@deloitte.ca
+1 4166016734

Global Coordination Team

Roel van Rijsewijk
Partner Cyber Risk Services
RvanRijsewijk@deloitte.nl
+31 882881103

Peter van Nes
Junior Manager Cyber Risk Services
PvanNes@deloitte.nl
+31 610042150

Mike Lameree
Senior Consultant Cyber Risk Services
MLameree@deloitte.nl
+31 610999190

Dana Spataru
Senior Manager Cyber Risk Services
DSpataru@deloitte.nl
+31 682019491