What Every CEO Needs to Know About Cybersecurity

Decoding the Adversary

AT&T Cybersecurity Insights | Volume 1

Contents

For more information:

Follow us on Twitter @attsecurity

Visit us at:

Securityresourcecenter.att.com

Business leader,

Welcome to the inaugural issue of AT&T Cybersecurity Insights, a comprehensive look at our analysis and findings from deep inside AT&T's network operations groups, outside research firms, and network partners. This first issue, "Decoding the Adversary," focuses on whether or not you and your board of directors are doing enough to protect against cyber threats.

Security is not simply a CIO, CSO, or IT department issue. Breaches, leaked documents, and cybersecurity attacks impact stock prices and competitive edge. It is a responsibility that must be shared amongst all employees, and CEOs and board members must proactively mitigate future challenges.

This first report is intended to help strengthen your cybersecurity management and awareness. It provides insights into current threats, evolving technological and operational challenges, and offers suggestions to help you initiate improvements in your organization, including:

- Enforce an action plan to ensure there's a consistent risk assessment process in place
- Better understand what data is leaving your company and why you might be a target for an attack
- Ensure clear understanding of which board committee is responsible for security
- Determine if your security team has necessary resources to protect against a breach

AT&T is committed to helping you understand where threats originate and how to formulate a business strategy for today's fast-evolving security environment. Future reports will cover topics including the Internet of Things, mobile devices, virtualized security, and other emerging trends. We will also publish ongoing and timely cybersecurity news and insights on our Security Resource Center (securityresourcecenter.att.com).

Thank you for the opportunity to share our leadership, knowledge, and experience in security with you.

John Donovan
Senior Executive Vice President
AT&T Technology and Operations

AT&T is committed to helping you understand where threats originate and how to formulate a business strategy for today's fast-evolving security environment.

Executive Summary

What every CEO needs to know about cybersecurity

Many executives are ill-advised and unprepared to tackle cybersecurity challenges.

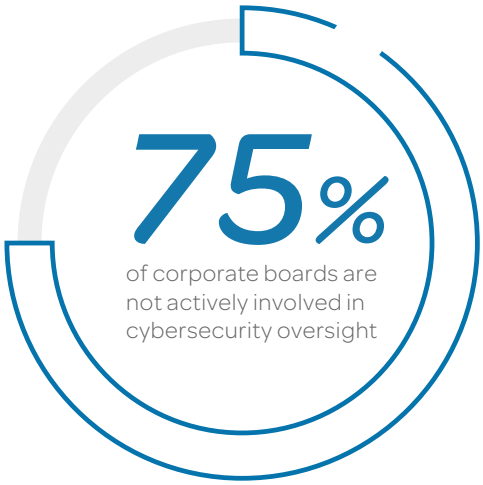
Status quo is not an option:

- Businesses suffered nearly 43 million security incidents in 2014, an increase of 48% over 2013 and equaling some 117 thousand incoming attacks daily[1]
- AT&T saw a 62% growth in DDoS attacks across our network in the last two years[2]
- 75% of businesses do not involve their full boards of directors in cybersecurity oversight[3]

Drawing upon decades of experience serving customers with one of the largest global IP networks, AT&T offers insights into technological and operational gaps where attacks occur. The goal is twofold: partner decision makers with those who implement cybersecurity actions and help leaders understand and implement tactics to guard from inevitable assaults.

Breaches and data loss headlines lower your company's reputation. As brand equity becomes intertwined with business results, board members and CEOs are accountable. However, security is a responsibility that must be shared amongst all employees.

The threats are pervasive. The need for action is clear. CEOs and board members must mitigate cybersecurity risks conjointly through proactive engagement.



Five questions every CEO should ask about cybersecurity:

1. *Is your board of directors fully engaged in cybersecurity?*
2. *When did you and your board review your last risk assessment?*
3. *What makes you a target for attacks?*
4. *What data is leaving your company and is it secure?*
5. *Have I provided my security organization all the tools and resources they need to help prevent a security breach?*

Introduction

In this section:

AT&T has unparalleled visibility to cyberthreats

Executives need security insights and details to build best practices

Bottom line: Make cybersecurity everyone's responsibility, including the executives

AT&T aims to arm you with information and best practices for elevating security in your organization to a strategic business imperative. We have unparalleled visibility into the data traveling over our network because we analyze over 10 petabytes of traffic each and every day. We're in a unique position to provide information and suggest best practices to elevate strategic security decisions.

This report — the first in a series we are calling AT&T Cybersecurity Insights — focuses on the adversaries attacking from inside and outside your organization.

The Center for Strategic and International Studies put the cost of cyberattacks to the world economy at around $445 billion,[4] or almost 1% of global income. Even at the low end of the range, that considerable figure is more than the national income of most nations and governments.[5]

Supporting a global network, we see increasing attacks against a variety of organizations. We have seen a 62 % growth in DDoS attacks across our network in the last two years.[6]

We have also seen a dramatic 458% increase in Internet of Things (IoT) vulnerability scans against devices.[7] A scan is an adversary looking for a weakness in your network defenses. The cost per security incident keeps rising. Organizations reporting financial hits of $20 million or more increased 92% over the number in 2013.[8]

Worldwide spending on information security was expected to reach $71.1 billion in 2014. Total information security spending is expected to grow 8.2% in 2015, reaching $76.9 billion.[9]

According to a recent survey,[10] nearly half of large companies are re-evaluating their information security standards as a result of high-visibility data breaches.[11] But that leaves 51% of large companies who are not. That indicates that many are lulled into a false sense of security or are willing to gamble that cyberattackers will overlook them in favor of richer targets.

IT and business leaders want insights into the motives and methods of specific attackers to better prepare their defenses. We organized this report around threat sources: outsiders, including organized criminal groups and nation-states with political goals, and insiders both malicious and unintentional. This report offers some ideas on how to leverage that new knowledge.

Know the Terms:

IoT (Internet of Things)

Connection of everyday objects with embedded electronics, from smartwatches to pet collars to cars, across modern networks.

DDoS (Distributed Denial of Service)

An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Outsider Threats

In this section:

Defense today requires an action plan centered on a strategic approach based on prevention, detection, and response

87% of U.S. business executives are worried that cyberthreats could have an impact on their company's growth prospects[12]

Bottom line: External attacks not only impact bottom lines and operations, but carry a personal impact for executives

In late January 2014, a large U.S. health insurance company discovered that cyberattackers had broken into the company's IT system. Foreign hackers were suspected of stealing personal information belonging to 80 million people in one of the largest heists of medical-related customer data in U.S. history.[13]

Unfortunately, that wasn't the end of the story. The insurer soon learned[14] that the attackers had infiltrated its network at least six weeks earlier, scooping up information useful for personal identity theft while monitoring the company's internal processes. What's more, investigators believe that the breach was part of a broader systemic campaign that included cyberattacks on several other major American companies.

Welcome to the new normal. Businesses now find themselves squaring off against cyberthreats from multiple elusive outsiders, ranging from cybercriminals to hacktivists to nation states. Experts describe this situation as a state of war.[15]

80 million

people had their personal information stolen in a cyberattack against a large U.S. health insurance company

Corporate Espionage: Industrial Cyberspies

The U.S. Government[16] now says cyberespionage is a significant and growing threat to the nation's security and prosperity. Groups behind these operations share one goal: steal intellectual property from businesses.

Consider, for example, these cases:

- At one company, hackers allegedly stole the passwords of 7,000 employees while the company was in a trade dispute focused on its sales to a foreign country[17]
- Hackers stole 2,900 e-mails with more than 860 attachments around the time one U.S. company was negotiating deals with foreign businesses[18]
- Foreign groups attacked 10 major U.S. banks in 2014. J.P. Morgan indicated customer records of 76 million households were stolen[19]

7,000
passwords
of employees were stolen during a trade dispute

What are their intentions?

All information is valuable to somebody. Cyberspies usually seek a combination of intellectual property and general business information.

U.S. authorities have indicted five foreign agents for intellectual property thefts from companies including U.S. Steel, Allegheny Technologies, Westinghouse, and SolarWorld. This is the first time the United States has brought a case where it publicly charged state-sponsored cyberespionage as a motive. The charges highlighted the multi-pronged nature of many cyberespionage campaigns. Law enforcement groups find that cooperating with industry groups better addresses cyberspying. Sharing security expertise and information has proven to be the most effective prevention methods for this threat.

As U.S. House of Representatives sub-committee chairperson Dana Rohrbacher stated during a cybersecurity hearing, "the economics of cybertheft is simple: stealing technology is far easier and cheaper than doing original research and development."[21]

Hackers are also eager to acquire sensitive internal communications that offer insight into their target's strategy and vulnerabilities. Adversaries then leverage the stolen information to alter negotiations.

Verticals: Who's most at risk for cyberespionage?

"Every company in every conceivable industry with valuable intellectual property and trade secrets either has been compromised already or will be in the future,"[22] said Senator Joseph Lieberman.

Some, but not all, of the most popular vertical industry targets include:

Retail and Hospitality. Cyberattacks against retailers (Target, Neiman Marcus, TJ Maxx, and many others) make big headlines because personal financial information of millions of customers is stolen. Business travelers have been the focus of attacks in the hospitality industry.[23]

Healthcare, Pharmaceuticals, and Related Technologies. Healthcare services and medical devices rate among the fastest-growing investment sectors.[24] As such, the development of new drugs requires major investments in research and development. Any information that would provide rival firms with shortcuts would be coveted.

Military Technologies. U.S. military systems, aerospace and aeronautics technologies are of great interest to strategic rivals. Cyberspies are alleged to have stolen the designs for multiple U.S. advanced weapon systems, including the F-35 Joint Strike Fighter, F/A-18 Fighter Jet, and the Patriot Missile System.[25]

Clean Technologies. New energy-generating technologies and ways to reduce greenhouse gasses are targets for cyberespionage, including foreign hackers indicted by the U.S. government.

Advanced Materials and Manufacturing Techniques. Companies are working to develop new ways to create advanced manufacturing technologies that improve industrial competitiveness. Any intellectual property that provides a shortcut would be priceless to rivals eager to create and sell competing products without the expense of research and development.

"The economics of cybertheft is simple: Stealing technology is far easier and cheaper than doing original research and development."

Dana Rohrbacher
U.S. House of Representatives

Nation-States

On November 24, 2014, the co-chairman of Sony Pictures Entertainment arrived at the office to discover a warning on the computer screen. Written over the image of a fanged skeleton, it said, "We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data shown below to the world."[26]

It would go down as one of the most damaging corporate cyberattacks ever.

A shadowy group calling itself the Guardians of Peace[27] had broken into the company's computer networks and gained access to more than 38 million files. Over the next several weeks, the Guardians of Peace began posting confidential—and sometimes gossipy—emails, password lists, and other information about Sony's business online.

The cyberattack was seen as retaliation for Sony's backing of the movie *The Interview*, a satirical comedy about a fictional plot to kill North Korean leader Kim Jong Un.

38 million

files were accessed in the Sony cyberattack

North Korea has steadfastly denied any involvement with the Guardians of Peace but publicly praised the attack as a "righteous deed."[28] Although the identity of the creator of the Sony hack may remain in dispute, the episode shows the challenge to businesses finding themselves caught in a political or ideological cross fire.

What are their intentions?

Pilfering data. Stealing intellectual property. Establishing political dominance in a region. Harming a company's computer networks as a demonstration of force. These are among the goals of nation-state outsiders.

Security officials fear the theft of security clearance records from the U.S. Office of Personnel Management will be used to blackmail individuals to turn over secrets and steal more information.[29] Personal leverage of that type has been used for decades by spies, and digital record theft makes gathering information easier.

Don't forget about financial gain and theft of intellectual property. Some groups, such as the Guardians of Peace, are out for retribution.

For some, hacking amounts to cyberwarfare, a political tool which, when employed, is extremely effective at helping a nation-state achieve a geopolitical goal.[30] Turn that around, and you'll find nation-states using hackers to defend their homeland interests.

How do they threaten your business?

It's difficult to attach an exact dollar amount to cyberdamage, since the victims are often not even aware they've been attacked. The annual estimated average financial loss, per cybersecurity incident in 2014, was $2.7 million, up 34% from a year earlier.[31] Victims of highly publicized breaches routinely spend hundreds of millions of dollars to repair the damage caused by cyberattacks.

The FBI offered some technical details about the unique capabilities of the software used in the Sony attack. According to media reports,[32] the agency said that the malware overwrites all data on a computer's hard drive and prevents the system from booting up. This made it "extremely difficult and costly, if not impossible, to recover the data using standard forensic methods." This type of software can be used by any cyberattacker.

Organized Crime

In a widely cited 2012 analysis, criminologist Mike McGuire concluded that organized activity could be responsible for as much as 80% of global cybercrime.[33] The Mafia has gone digital, and other groups have joined them.

So why care about organized cybercrime? Because it can affect your business. First, organized cybercrime is about more than dollars. National security can be at risk because many international organized groups may work to harm companies for political and financial reasons. Second, as mentioned before, $445 billion in losses are amplified. For example, $1 million in stolen intellectual property can ripple into a multimillion-dollar advantage for the company that gets its hands on the stolen information.

A UN draft report found that digital criminals have established cybercrime black markets around the world. These are built on a "cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information."[34]

Know the Term:

Malware

A generic term for several different types of malicious code.

What are their intentions?

It's almost always financial gain for organized cybercrime syndicates. But it can be complicated.

Let's look at the Russian Business Network as an example. The RBN, as it's known, is considered to be one of the biggest and most sophisticated cybercriminal organizations in the world. Its origins are still uncertain, but its impact in the cybercrime world has been profound.[35]

Stolen data not used directly by cyberthieves go to one of many black markets. Darkode, a criminal underground market shut down by the FBI in 2015, included databases filled with Social Security Numbers, access to computer attack software, and software to control and pilfer Android phones.[36] Experts believe there are over 800 such marketplaces worldwide.

Security researchers also say the RBN has profited by being a shelter for other illegal activities, including phishing scams. Its methods, motivations, and supporters shift constantly. And it operates where law enforcement is weak or corrupt.[37]

How do they threaten your business?

Cybercriminals hunt for soft and lucrative targets to attack. Many have shifted their focus in recent years from individuals to businesses.

In the healthcare industry, the street value of stolen medical information is $50 per record, compared to $1 for a stolen Social Security number.[38] Breaches in the healthcare sector topped the Identity Theft Resource Center 2014 Breach List, with 43% of the incidents identified in 2014.[39] The fresher the data, the higher the value on the black market.

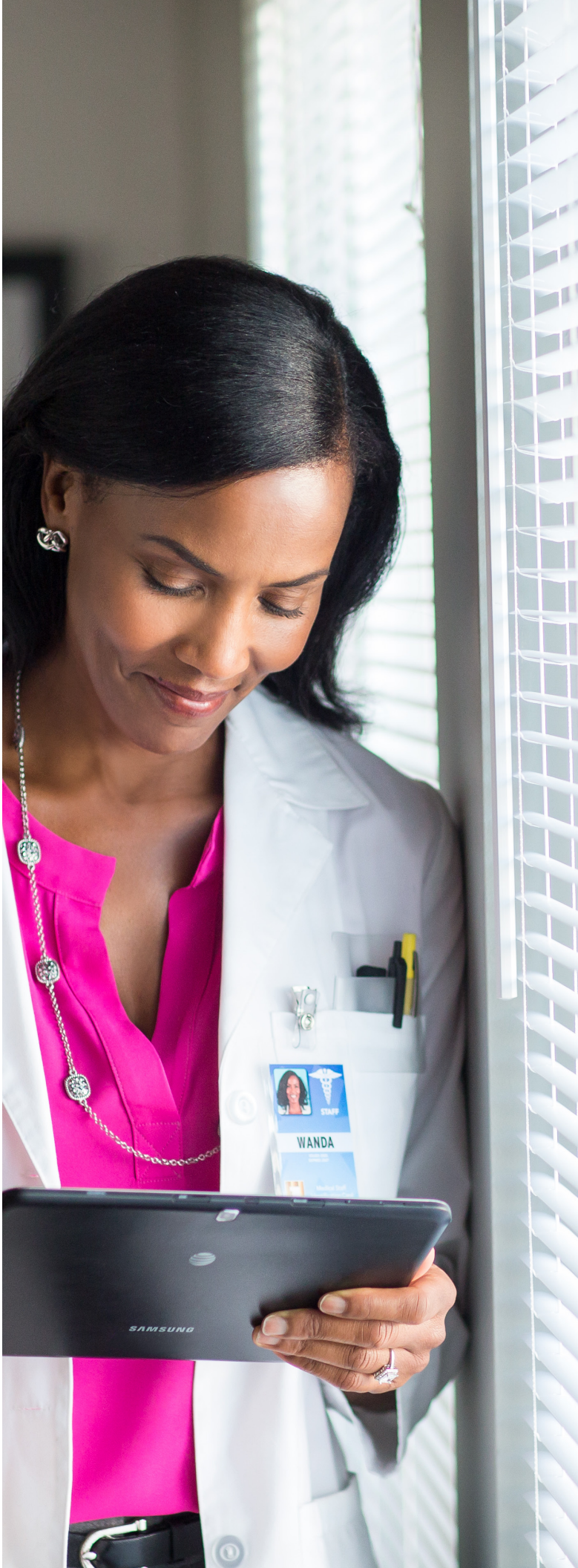
The financial services sector is a frequent victim, with 39% of the financial companies surveyed[40] reported being hit by cybercrime. That compares to 17% in other industries.

Other verticals targeted frequently by cybercriminals include education and government. Retailers also provide a perennial target[41] for cybercrime groups. Several of the hacked large retailers have spent hundreds of millions of dollars replacing credit cards and paying for credit monitoring services for their customers.

$50 > **$1**

Medical Record *Social Security Number*

The street cost of a stolen medical record is $50 compared to $1 for a stolen Social Security number



Types of threats:

Cybercriminals deploy a variety of methods to commit fraud or gain illegal entry into corporate networks. These include keystroke loggers, remote access Trojan viruses (software that hides inside innocent-looking apps then allows remote hackers to control a computer), phishing emails, and malware-infected websites. Software code inserted into a bank's ATM network spit out $2.9 million dollars in cash to criminals over eight hours in New York City in 2013.[42]

Cybercriminals are becoming increasingly sophisticated at social engineering. The wealth of information many people publish on their social media sites provides personal information that can be used by hackers to appear to be their friends. Repeated spear phishing attacks contain either an infected file or a link to an infected website. Unfortunately, humans continue to be weak points in company defenses.

Know the Terms:

Keystroke Loggers
Software that capture every key press, including usernames and passwords.

Spear Phishing
A targeted digital attack filled with personal information directed at a specific executive or company.

Hacktivists

The World Cup. Islamic extremists. The Philadelphia police department.

What do they have in common? They've all been targeted by the infamous group of hacktivists known as Anonymous.[43] Anonymous is a loosely connected group of unidentified hackers that first gained notoriety for a DDoS attack launched against the Church of Scientology in 2008.[44]

Hacktivists such as Anonymous are cyberintruders who use technology tools to promote social change or have an impact on public policy. They also tried to overload websites for PayPal, Visa and MasterCard after the companies refused to process donations to WikiLeaks.[45]

Moral issues now prompt attacks, such as the public hack and release of data from the Ashley Madison website.[46] A group calling itself the Impact Team hacked the site and threatened to release their stolen data unless the site closed. Avid Life Media, the owners of the site, refused to shut down, and nearly 10 gigabytes of customer information and internal emails have been released.

What are their intentions?

Pranks and practical jokes marked the early era of hacktivism, when participants operated more like cyber-street-artists than activists. Now, a political statement or act of cyberprotest is often the goal.

Hacktivists have been known to locate and publish a target's personal or corporate information, an act known as "doxing." In late 2011, for example, Anonymous successfully brought down the website of the private intelligence company Stratfor.[47] Stolen private data was then furnished to WikiLeaks.

The short-lived hacker group LulzSec said[48] that its 2011 attack against InfraGard was a response to reports that the Pentagon was thinking about classifying some cyberattacks as tools of war.[49]

"The new era of cybersecurity needs network data visibility at its core. Intelligence-driven threat detection and response can help organizations protect against a growing and unpredictable threat environment."

Todd Waskelis
AVP of Security Consulting AT&T

Know the Term:

Doxing

Searching for and publishing private or identifying information about a particular individual or entity on the Internet, typically with malicious intent.

Looking ahead: Outsider threats

According to a research study in 2014, 87% of US business executives are worried that cyberthreats could have an impact on their company's growth prospects, up from 69% the year before.[50]

Yet companies can still take a series of preemptive steps to improve their ability to prevent, detect, and respond to cyberthreats.

Success hinges on heightened awareness and engagement. Know your data, know your applications, know your users, and know your traffic.

If your monitoring software finds something unusual, handle it appropriately. If you don't conduct any business in certain parts of the world, block traffic from those regions.

Protect Your Business:

- *Perform a Data Inventory Analysis*
- *Share Internal & External Security Intelligence*
- *Authenticate and Authorize Users*
- *Analyze Data Traffic*
- *Verify Data Encryption*
- *Prepare for Multiple Attack Types*
- *Decide Who is Responsible for Data Security*
- *Look at Your Assets From the Outside*
- *Figure Out Where You Need Help*

Best practices: Outsiders

Companies can meet the threat challenge, but will need to shed outdated and reactive mind-sets. Defense today requires a strategic action plan centered on prevention, detection, and response.

Perform a Data Inventory, Data Valuation, and Data Risk Analysis. Request an inventory of the data your company protects. Once you know the value of that data, where it's located and the cost of loss to your organization, your cybersecurity defenses will become more focused.

Share Internal and External Security Intelligence. Demand more information sharing inside the company from the boardroom to every department and back. Participate in security working groups organized in your industry.

Authenticate and Authorize Users and Applications. Install two-factor authentication for important systems. Two-factor authentication creates another step of ID verification, an extra barrier between potential attackers and your data.

Analyze Both Inbound and Outbound Traffic. Verify what constitutes legitimate versus illegitimate traffic, and monitor the data flow in both directions. Monitor critical data closely to identify unauthorized access and removal.

Verify Data Encryption Usage. Ask your security team for an audit of current encryption practices. Data being transferred over the Internet outside the company, or stored outside the company, such as in cloud backup locations, should always be encrypted.

Prepare for Multiple Attack Types. The days when a single type of attack was the only threat factor are over. For example, a spear phishing campaign targets individuals but may leverage that point of entry to find other security gaps in your system.

Decide Who is Responsible for Data Security. Data security management tends to be split among multiple divisions. Some companies bundle data security under their IT or security teams. Others roll that oversight into the CSO or CIO role. Both approaches work, as long as security remains top-of-mind.

Look at Your Assets From the Outside. Appoint a group to evaluate what assets in your company most attract criminal scrutiny. Adjust your cybersecurity defenses accordingly.

Figure Out Where You Need Help. Figure out what expertise you need from external partners. Don't cling to the mistaken belief that you can do it all internally. There's no value in detecting a threat if you don't have the ability to respond properly.

Know the Term:

Two-Factor Authentication

A security process in which the user provides two means of identification: One is typically a physical token, such as a card. The other is typically something memorized, such as a security code.

"Cybersecurity is absolutely critical to the operations of any enterprise and executives need to pay as much attention to security as they do to the bottom line. A company's data has become as valuable as the products that company sells, so protecting that data is essential to having a viable business. It is imperative that corporate leaders and directors stay on top of security threats and ways to prevent them."

Ralph de la Vega
President and Chief Executive Officer
AT&T Mobile and Business Solutions

Insider Threats

In this section:

Employee cybersecurity knowledge is a key component of your defense

62% of cybersecurity professionals feel vulnerable to insider threats[51]

Bottom line: It takes one inadvertent click to expose your entire network to vulnerabilities

In June 2015, an employee at an Australian grocery chain sent an e-mail to 1,000 customers. Just doing their job, right?

But that e-mail mistakenly included an Excel spreadsheet with customer information and redeemable codes for close to 8,000 gift cards.

The result: The company had to cancel over $1 million in gift cards. Worse: customers' email addresses and names were exposed by the breach.[52]

Sometimes, your own employees or contractors can pose risks every bit as great as outsiders. In fact, some 32% of respondents to a global survey called insider crimes a *more* costly or damaging hazard than outsider threats.[53]

Malicious insider threats may be an employee, contractor, or vendor motivated by politics, revenge, greed, or basic corporate espionage. Unintentional risks created inside your company tend to be mistakes, such as someone opening a spear phishing email, plugging in a thumb drive that hasn't been security screened, or falling victim to a clever bit of social engineering by a smooth-talking con artist.

The cold hard reality is too many executives haven't given insider threats a second thought. Despite their legal responsibility for security,[54] many board members do not evaluate insider threat information. In this report, we highlight some of the most critical risks posed by insiders.

Malicious Insider Risks

No one could exactly put their finger on it, but there was something just a little, shall we say, fishy about one of the network managers working at the regional headquarters of a state government agency. When his superiors eventually asked AT&T to investigate, their worst fears were confirmed. For months he had been quietly sifting through his company's official databases for embarrassing information about people who tormented him in high school and was using it to blackmail them.

Revenge. Disgruntled employees can be a greater than expected menace. In 2012, for example, a technician at an oil and gas firm disabled all of the company's servers by returning them to their original factory settings shortly after discovering that he was about to be fired. He was eventually sentenced to four years in Federal prison and forced to pay $528,000 in restitution and fines, but only after the damage was done — at least $1 million to recover lost data, lost staff time, and costs for restoring those servers.[55]

Money. Criminals will pay insiders handsomely for confidential data. In one heavily publicized 2011 incident, an employee at a major financial institution sold customer information including names, bank account numbers, and PIN codes to outside criminal groups who subsequently used it to commit $10 million worth of fraud.

Whistleblowers. According to Ethical Systems, an ethical standards research firm, most whistleblowers act because they felt supported by managers and coworkers; they believed something would be done; and they were able to report anonymously. But sometimes, it is about the money. In 2014, for example, an insider whistleblower at a leading U.S. bank received $64 million from the Federal government for providing information about questionable mortgage insurance practices that led to a $614 million settlement with the Department of Justice.[56]

Hacktivism. Politically-motivated security attacks generally originate with outsiders, but Chelsea (nee Bradley) Manning, the soldier who disclosed hundreds of thousands of sensitive government documents to activist organization WikiLeaks, proved that activist insiders can do even more harm.[57]

Espionage. Patriotism, rather than greed, can inspire insiders, too. In 2011, for instance, a research scientist at a global chemical manufacturer pled guilty to sending $300 million worth of trade secrets to recipients in his native country.[58]

Business Advantage. Employees looking for a head start at a new job often take customer records and intellectual property with them on their way out the door. In some studies, as many as one in four people have admitted that they would attempt to take data even though they know it's against the rules.[59]

32% of respondents to a recent survey called insider crimes a more costly or damaging risk than outsider threats

Industry trends: Malicious insiders

Malicious insider threats impact every industry, but in different ways.

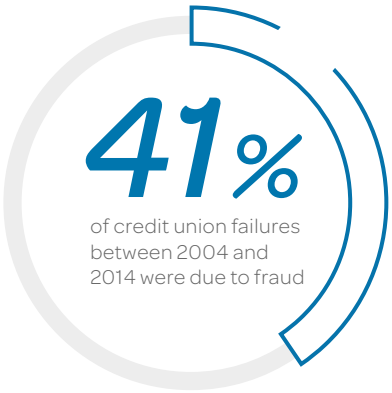
Financial services. Fraud is among the biggest insider risks faced by financial institutions. Employees at numerous firms have capitalized on poor security strategies to rob account holders and engage in insider trading. The consequences can be dire: Fraud contributed to 41% of credit union failures between 2004 and 2014.[60]

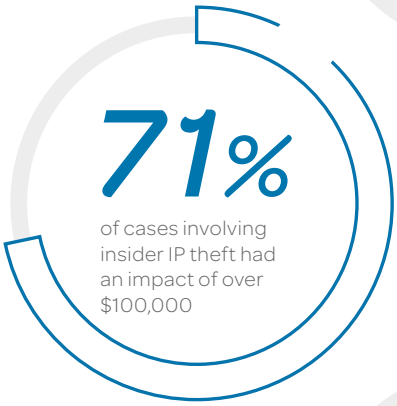
Manufacturing. Product designs, research and development projects, and other forms of intellectual property are tempting targets for ill-intentioned insiders. In one high-profile incident in 2013, a senior executive at a major computer chip manufacturer copied 8,148 files,[61] including top-secret licensing documents, onto a laptop shortly before resigning to take a job at a competing firm. When he walked out the door, he took with him years of work and research, and damaged the company's competitive abilities.

Retail. Major retailers, long subject to basic merchandise theft, now struggle with cyberattacks from within. Many of the most publicized hacks have highlighted the difficulty retailers have securing their large number of employees, both full and part time.[62]

According to researchers, insider theft of IP is significant. The impact was over $100,000 per incident in 71% of insider theft cases and over $1 million per incident in 48% of cases of IP insider theft.[63]

Government. Government insiders also engage in embezzlement and other types of fraud. In one case, two employees of the New York State Department of Motor Vehicles collected $1 million selling counterfeit drivers licenses to buyers who included people on the TSA's "no-fly" list. In another case, the treasurer and comptroller of Dixon, Illinois was convicted in 2013 of siphoning an astounding $54 million from public coffers over a 22-year period.[64]





Unintentional Insider Risks

The email certainly looked like the real thing. Received by a boutique financial services firm with high net worth clients, it included a long-time customer's name and email address. It sounded legitimate, filled with personal details. So when the sender concluded the message by requesting a $100,000 transfer to an overseas account, it never occurred to anyone to question it.

Until the *real* client called two weeks later wondering why all that money was missing.

The thief used a combination of a disguised email address and data gleaned from the client's social media accounts. That turned an experienced investment manager into an unwitting accomplice to a six-figure heist.

Intentional insider attacks grab most of the headlines these days, but incidents involving unintentional insiders can be just as dangerous. When asked by security analyst firm The Ponemon Institute in a June 2015 survey to name their employer's biggest user-based threat, 41% of respondents named negligence versus just 30% who cited malicious attackers.[65]

Know the Term:

Shadow IT

Third-party applications and other resources used by employees for business without IT department approval.

Shadow IT Use

Multiplying risks

Ironically, many of the same technologies and practices organizations are using to raise productivity and strengthen customer relationships are giving employees new ways to compromise security as well.

Shadow IT. A typical knowledge worker in your firm just wants to get her job done. And sometimes, the best way to do that is using a cloud-based application. She just opens a browser window, logs on and gets to work. The problem is, there's an 8 in 10 chance the Software-as-a-Service application that makes her so productive was not approved for use by her company and IT has no awareness or control over the data stored there.[66]

Mobility. Employees who place sensitive, unencrypted information on their mobile devices expose organizations to multimillion dollar regulatory fines and even more costly harm to their customer loyalty, intellectual

property, and public reputation. Bring Your Own Device policies are magnifying mobility-related risk by distributing data across a wider array of devices under less direct IT control. For example, lost or stolen laptops lead to 68% of the data breaches in the healthcare field.[67]

Social Media. Social media sites are powerful workplace tools for connecting with co-workers, business partners, and customers. Unfortunately, they're also convenient vehicles for accidentally broadcasting company secrets to a global audience. Spear phishing emails often contain personal information gleaned from social media postings.

Old-Fashioned Risks. Well-meaning insiders continue to compromise confidential data in more traditional ways. Employees still fall victim to phishing attacks, in which hackers use phony emails and websites to dupe unsuspecting people into exposing passwords, account numbers, and other valuable information. Some 31% of respondents to a recent cybercrime survey say their company fell victim to at least one phishing attack in 2014. Why? Nearly 40% of employees admit opening suspicious emails.[68]

End point risk

Short-term access, big-time risk

In June 2015 hackers stole data on 4.2 million current and former employees of the U.S. Office of Personnel Management. They hacked the system through a third-party that did background checks for the government.

Verify the security processes of your vendors.

While hiring temporary help can pay financial dividends those come with an unavoidable tradeoff in the form of heightened security dangers. Contract laborers can be an even bigger source of insider risk than full-time employees. Short-term workers typically have network accounts and access to sensitive data just like everyone else. But they're monitored less carefully, receive less security training, and often use devices brought from home or provided by a temp agency that are harder for IT to secure.

Industry trends: Unintentional insiders

Every industry experiences negligent insider hazards, but the type and degree of those risks can vary significantly. While smaller companies often believe they have less exposure, data accumulation has become an issue for every business in every industry. Customer transaction records, including regulated credit card data, quickly grow into databases filled with hundreds or thousands of megabytes.

Healthcare. Two facts explain why hospitals and insurers are among the most common victims of unintentional insider security incidents: Their databases are packed with confidential and highly-regulated patient records, and the doctors and nurses accessing those records generally have little security know-how and even less time to acquire it. Medical data is highly prized by phishing attackers,[70] who can use it to buy or steal drugs or file fraudulent insurance claims. Unlike credit card numbers, healthcare information is a durable resource. You can cancel a stolen credit card pretty easily, but canceling your medical history is nearly impossible.

That's why stolen health credentials can go for up to 50 times the value of a U.S. credit card number.[71] That contributes to the high cost of a data breach for healthcare.

Financial Services. Financial institutions are on the receiving end of even more phishing attacks than healthcare providers. Financial and payment services accounted for 59% of phishing attacks in 2014.[72] Lately, criminals have been more frequently targeting middle managers, who tend to be older and less tech-savvy than the Millennials working for them.[73]

Government. Federal, state, and local government agencies are especially avid users of contractors. The U.S. Department of Defense alone issued security clearances to almost a million people not on its full-time payroll as of 2014, according to a study by the U.S. Government Accountability Office.[74]

Technology Firms and Practices. Programmers often leave vulnerabilities in new code due to lack of review and testing time. Reused code from software built before more stringent security testing procedures can lead to trouble. IT administrators often create security gaps by creating software to perform jobs automatically, bypassing security controls, leaving default passwords on equipment, and deviating from security policies because of time constraints or taking short cuts.[75]

"Lifecycle support of systems and services is necessary. Find and get rid of old, unneeded systems."

Rich Shaw, Jr.
AVP Network Services AT&T

Looking ahead: New potential threats

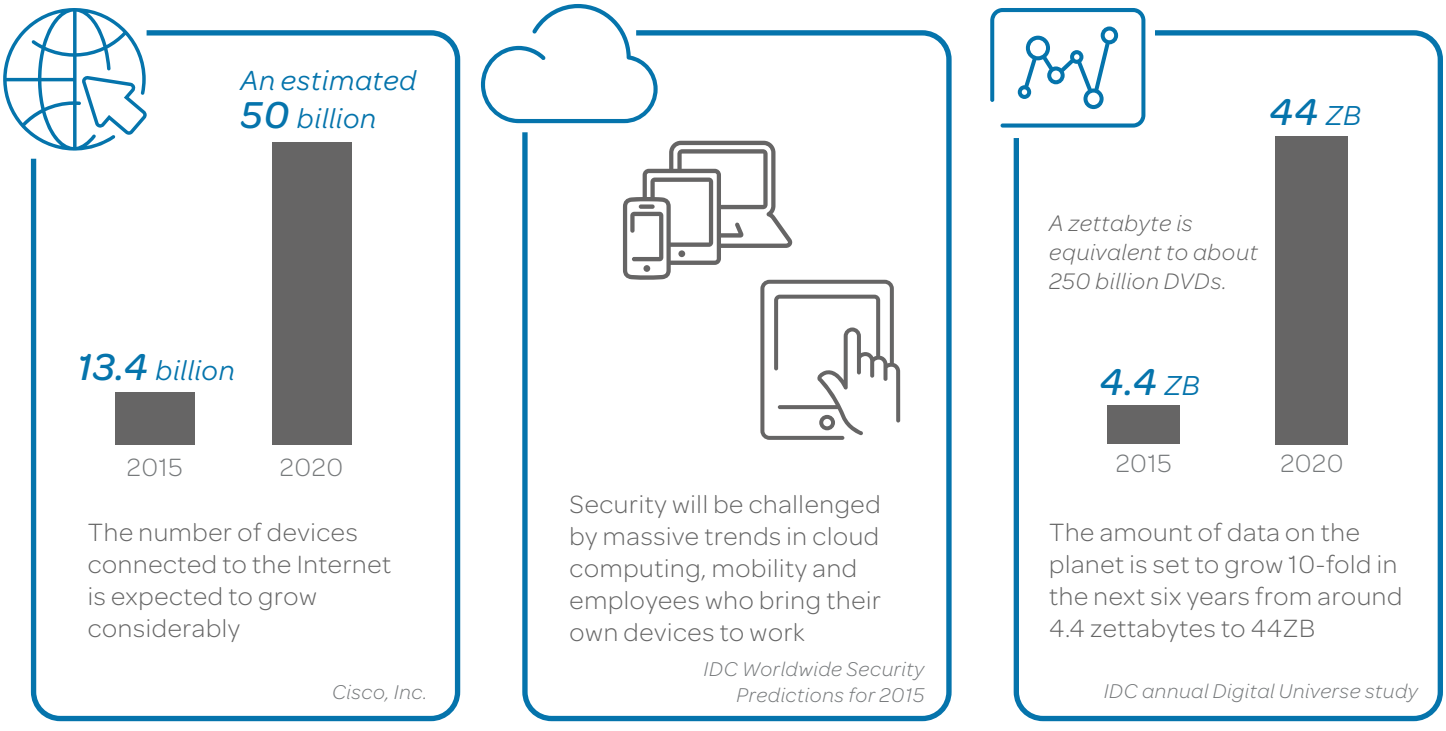
Several emerging technologies and trends are expected to give malicious insiders dangerous new avenues of attack in the future:

The Internet of Things. An estimated 50 billion "things" ranging from sensors in cars and traffic lights to utility meters and household appliances will be sharing data over the Internet by 2020. Data may grow tenfold to 44ZB over that time.[76] Those small sensors can be harder to secure than bigger, more sophisticated devices like PCs and tablets, and their growth will give malicious insiders a host of new ways to engage in sabotage and hacktivism. Bottom line: More but less complex devices mean more potential security gaps to manage.

Cloud Computing. Public cloud computing has become standard business practice for many businesses today, forcing you to rely on third party providers for part of your data security. The explosion of mobility and widespread use of personal devices for work asks you to balance the increased risk from user devices with the proven productivity benefits. Verify that all links to cloud storage and applications connect over secure and managed networks.

Mobility, and Bring Your Own Device (BYOD). The explosion of mobility and widespread use of personal devices for work will force you to balance the increased risk from all those devices with the proven productivity benefits.

Big Data. Although Big Data tools are already widely used within large organizations, the scale and number of Big Data deployments is set to grow enormously in coming years. Unfortunately, the tools those deployments rely on to distribute massive amounts of sensitive information have few built-in security safeguards, making them vulnerable to insider misuse.



Looking ahead: Emerging risks

Several developments over the years ahead will turn unintentional insiders into an even greater danger.

Extended Supply Chains. As businesses continually optimize their logistics, organizations are linking their internal business systems with their suppliers through the Internet. In the process, they're also putting more data in the hands of more insiders at more companies whose security practices and policies are beyond their IT departments' control.

Home Health Monitoring Devices. Home healthcare devices empower caregivers to shorten hospital stays and reduce emergency room visits by remotely monitoring recent patients and chronic disease sufferers. However, due to lack of understanding of proper security procedures, the user may create unintentional vulnerabilities when using these devices.

"There is a black market for data and information that leadership needs to be aware of. This underground trade has culminated into a large, adversarial economy. Cybersecurity strategy can't ignore this presence today or tomorrow as it will continue to grow."

Jason Porter
VP of Security Solutions AT&T

Best practices: Malicious insiders

Already a huge problem, malicious insiders will only grow more numerous and dangerous in the years ahead. These steps can help you combat them.

Strengthen Your Security Foundation. Focus your team on the basics first. A surprising number of organizations leave themselves exposed to internal threats simply by neglecting simple security practices. Cancel a departing contractor or employee's network privileges *immediately* after their last shift. Change passwords on systems the ex-worker accessed. Cancel their physical access cards or badges. Assign access rights to sensitive information on a need-to-know basis only.

Make Security Everyone's Responsibility. Employee training helps turn employees into a malicious insider early warning system. Adopt the "If you see something, say something," attitude for users, and reinforce that everyone follows security procedures. This responsibility also applies to all executives and board members.

Break Down Organizational Silos. Demand security teams have full access to all data and records in all departments and divisions. Hackers count on bureaucratic inefficiency and barriers between groups. Take that advantage back from the malicious insiders. Break down barriers by forming joint task forces and increase the ability to identify and eliminated insider threats.

Invest in Behavioral Analytics. Big Data tools can help sniff out activities by malicious insiders. Monitor user IT activity, look for abnormal patterns, and investigate suspicious actions. An employee arriving two hours earlier than usual may not be a coincidence.

Best practices: Unintentional insiders

In the case of unintentional insider risks, some of the most effective steps you can take involve changing policies and procedures rather than deploying new tools.

Train Your Users. Offering mandatory annual or semi-annual security awareness courses to teach people how to avoid phishing attacks and use social media safely, among other things, is a good starting point. And shockingly underutilized: Only half of the business and security executives surveyed in 2015 said they conduct periodic employee security training.[77]

Share the Security Responsibility. Follow the ISO 27001 recommendation to create a steering group that includes members from across your organization, including leadership. The "Information Security Management System Roles and Responsibilities"[78] is a good place to start. The National Institute of Standards and Technology also provides best practice guidelines.

Employee Buy-in for Security Starts at the Top. CEOs, board members, and top executives should lead by example. They need to embrace the policies, talk about them in ways employees will understand, and practice what they preach.

Enforce the Rules. Accompany your security training efforts with prompt and highly visible enforcement of your security policies in the form of fines, terminations, or both. Rules and policies around system access and authentication are critical.

Don't Ban Shadow IT. Manage It. Find out why business units buy cloud services on their own, and find more secure ways to address those issues. If getting new solutions through IT takes too long, for example, streamline your procurement process and accelerate application development.

Evaluate and Monitor Your Suppliers. Prevent a supplier's employees from endangering your data and intellectual property by assessing their security and compliance practices before and while doing business with them.

- *Train Your Users*
- *Share the Security Responsibility*
- *Employee Buy-in for Security Starts at the Top*
- *Enforce the Rules*
- *Don't Ban Shadow IT, Manage It*
- *Evaluate and Monitor Your Suppliers*

Moving Forward

In this section:

Business and security alignment is as important as business and IT alignment

Managing reputational, operational, and financial risks is important to a successful security environment

Bottom line: New technologies have transformed everything in business security and risk management

Technologies have improved and transformed your business processes. Cloud computing, mobility, Bring Your Own Device (BYOD), social media, and Big Data have reduced the friction that once slowed business. They have erased the boundaries between your company and the world. Information technology departments and business executives have been drawn together like never before to enable these new technologies.

The growing wave of connected devices is fueled by the dramatic drop in the cost

of networked sensors. This means better monitoring and management of a wide number of devices and work processes. But this also means your network will add thousands of low-cost products with little capacity for complex security software. Cyberdefense for IoT will live inside the network architecture and require rethinking endpoint defense.

Moving forward, every enterprise must rethink their place in today's connected world. But too many business leaders are unaware of just how much has changed and how tempting their company may now be to cyberattackers. Consider the construction company whose board reasoned they were not a target since they didn't keep credit card information like a retailer. Their security adviser asked about their 50,000 employees, each with a Social Security number. And the company had a large bank account, stored payroll information, and Intellectual property. They were definitely a target.

Making the Case

"Elevate security to where it belongs, top of mind and top down. Boards and senior leadership must work to close the gap between themselves and their cybersecurity team. Tight alignment is critical to building and executing a successful strategy."

Jason Porter
VP of Security Solutions AT&T

Here's part of the problem: Too often security remains one step removed from the officers and directors of the company. Security is seen as a technology issue. But security is first and foremost a *people* issue.

The good news is that more security leaders report directly to a C-level officer.[80] This will help elevate security to where it belongs: top of mind from the top down.

Tools to improve security alignment

No enterprise can afford to turn away from the promise of social, mobile, Big Data and the cloud. CIOs have made giant strides in aligning IT with business needs. Now boards of directors, officers, and business executives need to find common cause with security leaders so that it becomes everybody's job to align security with business.

Here are the AT&T Keys to security/business alignment in tomorrow's security landscape:

Culture. Security needs to be a cultural pillar that is promoted, practiced, and valued from the top down. Training is one way to promote security awareness into employee culture.

Planning. Business goals should be shoulder-to-shoulder with security strategy driving technology and business decisions; risk, governance, and compliance are key ingredients in all decision-making. The earlier security enters the planning the process, the more secure the result.

Toolset. Services and solutions need to be in place to protect and defend against breaches. Leaders should become conversant with umbrella technical terms like threat management, layers of security, cloud-based management services, and the modern advanced perimeter defense that drills down to individual device protection. These tools can be controlled internally or in cooperation with external partners. Your IT leaders have hardware options (firewalls), software tools (intrusion detection, anti-virus, email gateways, mobile device management), and policy systems (defense in depth) available. Security managed service providers or consulting organizations can help you fill any tools gap, and benchmark your cyberdefenses against comparable companies.

Partnerships. Identify the security stakeholders and sync them to a common goal across the organization. Security/business alignment depends on these relationships.

Financial Support. Ensure security spending is a priority. Policy and spending decisions are determined by risk, security, intelligence, and data.

There's a lot at stake. The infamous 2013 attack on Target has cost the company $162 million and counting. That does not include the damage to Target's reputation or the lives of the executives who have lost their jobs.[81]

The basics of cyberrisk management

As a business leader, you make risk decisions on a daily basis: Should you invest in a new market? Should you launch a new product? But how often do you ask, "Is entering this new market going to expose our business to cyberrisks we may not be able to defend against?"

Honestly, most executives are not equipped with the information to properly answer that question, but they need to educate themselves, and they need to do so quickly.

The reality is that every single business or organization, no matter how large or small, is a target for cyberattack. From a business standpoint, risk associated with cyberattacks takes on many forms:

Reputational. The damage to your company and brand caused by a cyberattack.

Operational. Your ability to continue operations in a manner determined by the business leaders.

Financial. Loss of customer revenue and the cost of replacing lost customers, for starters, followed by fines levied by regulators, costs of remediation, legal fees to resolve class-action lawsuits and the need to deal with government actions that may hit soon after the breach.

Liability. Inherent liability of damages resulting from the cyberattack.

AT&T Keys to Cyberrisk Management:

How to spot the risks. What are you doing that increases your risks, and what are you doing about that?

How to assign value to those risks in terms of impact on the business, both financially and operationally. A focus on data here is critical—what do you have, where is it, and what is it worth?

How to know the downside. What are the ranges of outcomes from cyberrisks?

How to address those risks. How do you handle mitigation, avoidance, acceptance, and insurance?

"Proper cybersecurity starts with effective cyber fundamentals."

Dr. Tina Hampton
AVP of Security Innovation AT&T

Conclusion

Your Call to Action

You should now understand why we say that threats are pervasive. CEOs and board members must mitigate cybersecurity risks conjointly through proactive engagement. Here are some best practices for you to follow to help secure your organization today and into the future.

Make Sure This is Understood: Security Is Your Responsibility. Officers and directors have a fiduciary obligation to run their companies with reasonable care. In carrying out these obligations, "officers and directors must assume an active role in establishing the correct governance, management, and culture for addressing security in their organization."[82]

Adopt a More Risk-driven Approach. You need to have a good handle on the damage cyberattacks can do to your bottom line and reputation. Ask your IT group when it last performed a full risk assessment and evaluation of brand asset protection.

Appoint Someone to Champion Data Security. Data security needs a strong advocate. Companies place that responsibility under various positions, usually within their IT or security groups. This approach best provides data security feedback to leadership.

Form an Information Security Committee. Make this group responsible for the design, implementation, and day-to-day oversight of cybersecurity compliance efforts. This will promote information sharing inside the company—especially at the executive and director levels. Regular communications between business and security leadership improves cybersecurity.

Evolve with Technology. Creating a security infrastructure is not a one-time project. Continuing to invest in capabilities that respond to evolving adversaries will better protect your business and brand equity moving forward.

Get Outside Help. Outside advisors will, ideally, offer a more holistic and objective security perspective. You know your company but an outside security consulting group knows the security practices of many companies.

Lead by Example. Don't let security policy exemptions become a perk for directors and officers. They're not a perk—they're a weak link and the reason executives attract spear-phishing attempts. If you use encryption, secure log-ins and strong passwords and go through security audits like everyone else, your peers and employees will see you're all in for security—a powerful message.

Your adversaries are evolving. Your cybersecurity strategies must adapt to protect your business. Your employees, your reputation, and your shareholders are counting on you.

Know the terms

Cybersecurity terms evolve. This glossary details the terms and their definitions as used in this report and other commonly referenced materials.

APT (Advanced Persistent Threat)
A targeted attack by adversaries that penetrate a network without detection, maintains access for a period of time, all while monitoring information or stealing resources. APTs require considerable resources and may continue for years.

Authentication
The process of confirming the identity of a user, most often with a username and password.

Black Hat Hackers
An individual with extensive computer skills used to breach security of companies for malicious purposes.

Botnet
A large number of compromised computers used to create and send spam or viruses, or flood a network with messages such as in a distributed denial of service attack.

Botnet Management
Command and control tools that allow hacker groups to manage huge numbers of compromised systems.

Data Mining
A technique used to analyze existing data for enhanced value.

DDoS (Distributed Denial of Service)
An attack to make an online service unavailable by overwhelming it with traffic from multiple compromised systems.

Defense In-Depth
The approach of using multiple layers of security to maintain protection after failure of a single security component.

Doxing, Doxxing
Broadcasting personal information about a person or group, usually done by Internet vigilantes or hacktivists. The term comes from "dropping dox" using the slang term for .DOCX, the file extension used by Microsoft Word.

Encryption
Translating data into unreadable code to keep that data private. See Public Key Encryption for more.

Firewall
A hardware or software system that blocks unauthorized traffic from entering (or leaving) a network.

Gamers, Kids, and Amateurs
In the mid-1990s, cybervandals defaced Web pages operated by the early generation of online businesses. These so-called script kiddies were an annoyance but did little damage. They've since given way to a new class of attacker with more sophisticated software tools and ambitions.

Grey Hat Hackers
Ethically between black hat and white hat hackers, grey hats exploit system vulnerabilities, which is technically illegal. They tend not to leverage these hacks as a criminal, but sometimes offer to close the security gap for a fee.

Hacktivist
Hacker or group that breaches systems for political, rather than monetary, gain.

IoT (Internet of Things)
Connection of everyday objects with embedded electronics, from smartwatches

to pet collars to cars, with each other across modern networks.

Keystroke Logger, Keylogger
Surveillance software that records every keystroke, including usernames and passwords.

Malware
A generic term for a number of different types of malicious software. A malware payload may be delivered by a virus, via email, or compromised website page.

Packet
A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data.

Phishing
Social engineering through emails using known information about the target to acquire other data such as user names, passwords, or financial information.

Public Key
The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

Public Key Encryption
Encryption system that uses two mathematical "keys." One, the public key, is known to everyone and used to encrypt a message. The second, the private key, is known only to the recipient and used to decrypt a message.

Shadow IT
Third-party applications and other resources used by employees for business without IT department approval.

Spear Phishing
A targeted digital attack filled with personal information directed at a specific executive or company.

Two-Factor Authentication
A method used to improve security by requiring two separate items for access to a resource. These usually include something the user knows (password or PIN), something a user has (access card), or something attached to the user (fingerprint or retina to scan).

Trojan, Trojan Horse
Malware that appears to be a benign and useful application to encourage users to run the program, which installs the destructive payload.

White Hat Hackers
Computer security experts who penetrate networks to warn companies of gaps that a malicious attacker could exploit. They are often employed by the companies themselves to test the durability of their systems.

Zero-day Attack, Zero-day Exploit
A computer threat that tries to exploit computer application vulnerabilities that is unknown to others or undisclosed to the software developer. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software developer knows about the vulnerability. A cyberattack that exploits a vulnerability the day it becomes known, or even before vendors are aware they have an issue. Hackers then take advantage until users apply a patch to close the security hole.

End notes and sources

1 PwC Global State of Information Security Survey 2015

2 AT&T Security Operations Center

3 PwC US State of Cyber Security 2015

4 Net Losses: Estimating the Global Cost of Cybercrime," Center for Strategic and International Studies, June 2014

5 http://knoema.com/nwnfkne/world-gdp-ranking-2015-data-and-charts

6 AT&T Security Operations Center

7 AT&T Security Operations Center

8 PwC Global State of Information Security Survey 2015

9 http://cybersecurityventures.com/cybersecurity-market-report-q2-2015/

10 IDG "State of the CSO" survey 2015

11 Ibid

12 PwC 2015 "Progress Stalled" Cybercrime Report

13 http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html

14 Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, D.C.,

15 https://www.jpmorgan.com/tss/General/Cybercrime_This_Is_War/1320514323773

16 http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

17 http://www.technologyreview.com/featuredstory/538201/cyber-espionage-nightmare/

18 Ibid

19 http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372

20 http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

21 Sub-committee chairperson Dana Rohrbacher of the U.S. House of Representatives, United States House (2011-06-30). Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology

22 Floor Statement for Sen. Joseph Lieberman Introduction of Cybersecurity Act of 2012

23 http://www.securityweek.com/darkhotel-attackers-target-business-travelers-hotel-networks

24 http://ita.doc.gov/td/health/medical%20device%20industry%20assessment%20final%20ii%203-24-10.pdf

25 http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/

26 Sony Hackers Seen Having Snooped for Months, Planted Bomb," http://www.bloomberg.com/news/articles/2014-12-19/sony-hackers-seen-having-snooped-for-months-planted-bomb

27 https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

28 http://www.theguardian.com/world/2014/dec/07/north-korea-sony-hack-a-righteous-deed-but-we-didnt-do-it

29 https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html

30 http://www.darkreading.com/risk/why-russia-hacks/a/d-id/1318733?ngAction=register

31 CSO-PricewaterhouseCoopers Global State of Information Security, 2015

32 http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202

33 http://dev.defense-update.com/20120328_organized_cyber_crime.html

34 Comprehensive Study on Cybercrime," United Nations Office on Drugs and Crime, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

35 http://www.newsweek.com/russian-computer-hackers-are-global-threat-75837

36 http://money.cnn.com/2015/07/15/technology/darkode-shutdown/

37 IDC Security Products and Services group.

38 The World Privacy Forum

39 http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

40 "Global Economic Crime Survey," 2014, http://www.pwc.com/gx/en/economic-crime-survey/

41 https://www.trustwave.com/trustednews/2013/02/trustwave-reveals-increase-cyber-attacks-targeting-retailers-mobile

42 http://www.theatlantic.com/technology/archive/2013/08/productivity-tools-for-cybercrime/278974/

43 https://www.youtube.com/user/AnonymousWorldvoce

44 http://www.cnet.com/news/anonymous-hackers-take-on-the-church-of-scientology/

45 http://www.aljazeera.com/news/europe/2010/12/201012916376458396.html

46 http://www.cnbc.com/2015/08/18/hackers-post-stolen-ashley-madison-user-data-report.html

47 http://venturebeat.com/2011/12/28/anonymous-stratfor-hack-10-things-to-know/

48 http://www.digitaltrends.com/computing/lulzsec-hacks-fbi-affiliate-infragard/

49 http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html

50 PwC "Progress Stalled"

51 http://www.reuters.com/article/2015/06/18/dc-crowd-research-idUSnBw185371a+100+BSW20150618

52 http://www.darkreading.com/attacks-breaches/woolworths-self-inflicted-breach-a-clear-example-of-insider-negligence/d/d-id/1320658

53 PwC's 2014 U.S. State of Cybercrime Survey

54 Interview with M. Overly, Foley Lardner LLP, 8/10/15

55 http://www.pcworld.com/article/2158020/it-pro-gets-prison-time-for-sabotaging-exemployers-system.html

56 http://www.justice.gov/opa/pr/jpmorgan-chase-pay-614-million-submitting-false-claims-fha-insured-and-va-guaranteed-mortgage

57 https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html

58 http://www.ibj.com/articles/22011

59 https://www.sailpoint.com/blog/2014/12/2014marketpulsesurvey/

60 National Credit Union Administration

61 http://litigator110.rssing.com/chan-13817333/all_p1.html

62 http://www.ft.com/intl/cms/s/2/d2e5f3b6-43c8-11e4-baa7-00144feabdc0.html#axzz3jqZ6XHju

63 https://insights.sei.cmu.edu/insider-threat/2013/12/-theft-of-intellectual-property-by-insiders.html

64 http://articles.chicagotribune.com/2013-02-15/news/ct-met-rita-crundwell-sentencing-0215-20130215_1_comptroller-rita-crundwell-mayor-james-burke-fraud-scheme

65 http://www.ponemon.org/local/upload/file/2015%20State%20of%20Endpoint%20Risk%20FINAL.pdf

66 http://research.gigaom.com/report/shadow-it-data-protection-and-cloud-security/

67 2014 Bitglass Healthcare Breach Report

68 http://www.softwareadvice.com/security/industryview/phishing-scams-report-2015/

69 http://www.ponemon.org/local/upload/file/2015%20State%20of%20Endpoint%20Risk%20FINAL.pdf

70 http://www.ihealthbeat.org/insight/2014/health-care-industry-to-see-phishing-malware-attacks-intensify-in-2015

71 http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

72 http://www.statista.com/statistics/266161/websites-most-affected-by-phishing/

73 http://www.csoonline.com/article/2937146/malware-cybercrime/phishers-target-middle-management.html

74 http://www.washingtonpost.com/politics/federal_government/dod-has-1-million-contractors-eligible-for-security-clearance-but-not-on-payroll/2014/09/21/1a94a4fe-402d-11e4-b0ea-8141703bbf6f_story.html

75 http://www.slideshare.net/DrShawnPMurray/murray-insider-threat

76 http://idcdocserv.com/1678

77 PwC US State of Cyber Security 2015

78 http://www.iso27001templates.com/files/isms05001-information-security-roles-and-responsibilities-v1r0-draft-1.pdf

79 IDC Reveals Worldwide Security Predictions for 2015," IDC, Dec. 11, 2014

80 IDG "State of the CSO" survey, 2015

81 http://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/

82 http://www.foley.com/taking-control-of-cybersecurity-a-practical-guide-for-officers-and-directors-03-11-2015/