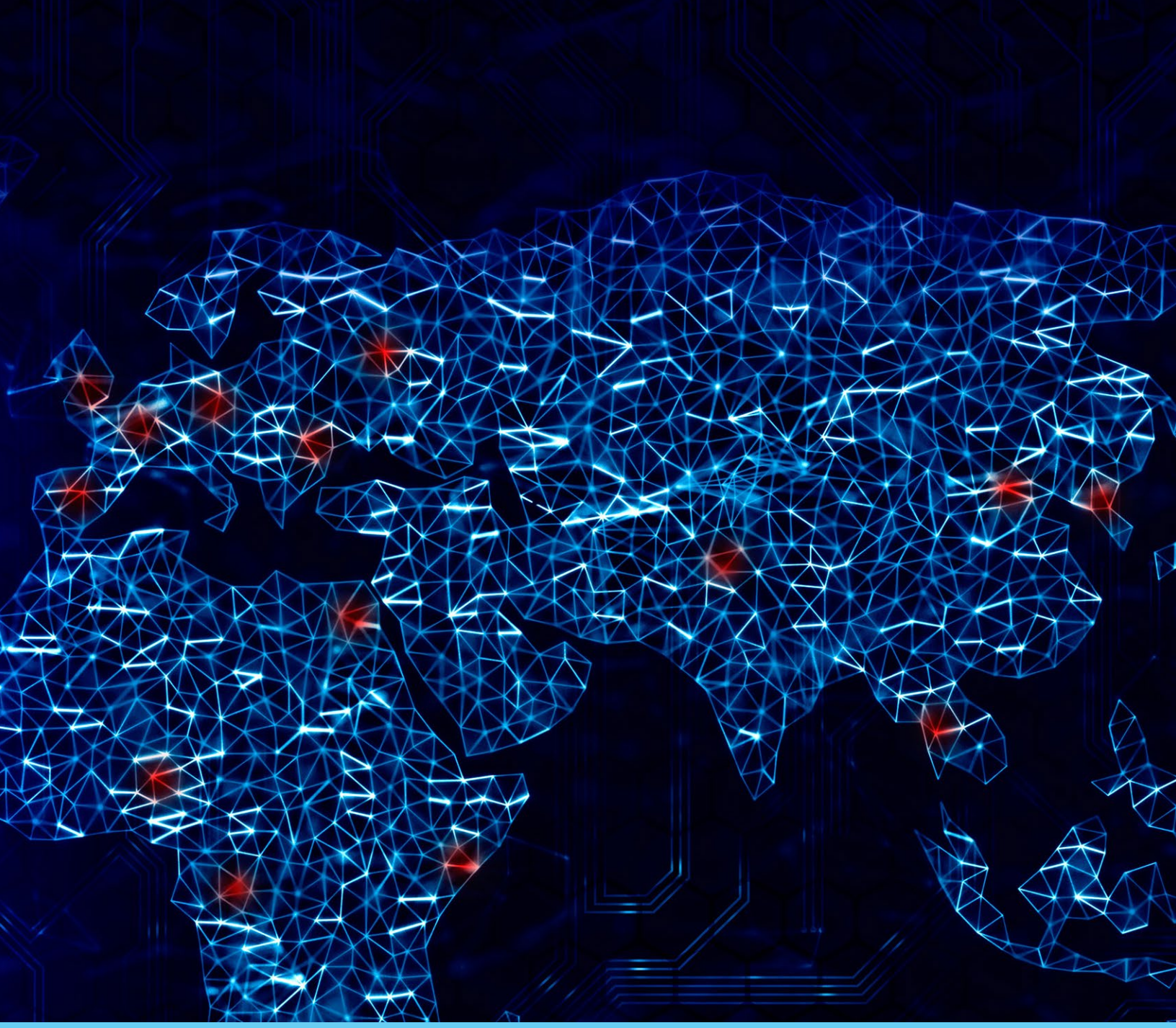
# The CEO's Guide to Navigating the Threat Landscape

*Keeping a step ahead*

AT&T Cybersecurity Insights | Volume 4



More than **90%** of attacks logged by AT&T are known attacks or their variants – not zero-day attacks.

# Contents


*4 Executive summary*

*5 Navigating the known threat landscape*

6 Malware

8 Ransomware

8 Advanced persistent threats (APTs)

10 Distributed denial of service (DDoS)

12 Fighting the knowns

*13 What's next: Emerging vulnerabilities*

14 Internet of Things

14 Cloud technology

16 Mobile devices

*18 Priorities for the year ahead*

18 Risk and vulnerability assessments

21 Tools: A shift toward automation

22 Awareness and training: Not one and done

*24 Conclusion: Your call to action*

*25 Additional reading*

*25 About our survey*

*26 Endnotes and sources*


***For more information:***

Follow us on Twitter @attbusiness

Visit us at

securityresourcecenter.att.com


© 2016 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T Globe logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.


# Executive summary

Cutely named cyberthreats like Poodle, Bart, and Locky may sound harmless, but they could cost your business millions. The FBI estimates that ransomware, for example, is on track to become a $1 billion crime in 2016[1]. A Russian cybercriminal gang allegedly used malware called Lurk to steal $45 million from financial institutions and other organizations over the course of several years[2].

The vast majority of these threats are well known. Our threat intelligence data tells us that more than 90% of the attacks we see across our networks are known threats or variants of known threats — not zero-day attacks resulting from previously unknown holes in software. The tools and skills needed to help protect against most of these cyberattacks are readily available.

So why aren't organizations doing a better job of protecting their assets?

Part of the challenge is the increasing volume of cyberattacks. The mainstreaming of threat methods has made it easy for anyone — from a nation state to a bored high school student — to launch an attack on your organization. They search for weak spots to exploit across your workforce, your partners, and your IT systems. AT&T intercepts thousands of malicious emails daily. It only takes one, opened by an unassuming employee, to deliver a dangerous payload that can lock up your systems or lurk undetected while criminals steal valuable data.

Adding to the challenge, widespread adoption of emerging technologies such as the Internet of Things, cloud technology, and mobile devices provide new points of entry for cybercriminals to exploit using tool kits easily acquired on the Dark Web, an alternative gateway to information and communication on the internet.

Many cybersecurity pundits focus on the fear of the unknown. But we believe organizations are better off focusing on the knowns: the documented forms of malware and commonly used tactics that make up the vast majority of cyberattacks.

By remaining true to foundational security practices, while recognizing the distinctive risks of emerging technology, you can detect and respond to the majority of cyberattacks your organization encounters each and every day.

When planning for the year ahead, cybersecurity priorities should include:

**Risk and vulnerability assessments.** Knowing what you need to protect and where your vulnerabilities exist are critical first steps in a comprehensive cybersecurity strategy.

**Automation tools.** Stay focused on the basic detect-and-respond defenses required to help protect against known threats. The rising volume of known threats also requires a shift toward automated technologies that help improve the pace and scope of your response.

**Awareness.** Employee awareness training and governance policies must be regularly refreshed to keep best practices top of mind among all constituents.

We aren't suggesting that you should ignore the emerging unknowns of the threat landscape. But by defending against the most prevalent and well-known forms of attack — using established practices and commonplace protection tools — your organization will be a less attractive target for cyberattacks in 2017 and beyond.

## *Spotlight on security*

- **Build your defenses around known threats**
- **Foster a cybersecurity culture within your organization**
- **Keep current with security patches, logs, and software updates**
- **Implement new technologies with security in mind**

# Navigating the known threat landscape


*In this section:*

**Malware:** 90% of U.S. organizations had at least one malware-related incident during the past 12 months[3].

**Ransomware:** 63% of organizations were confronted with at least one ransomware incident over the past 12 months[4].

**APTs:** 65% of survey respondents in the financial services industry had an APT-related incident over the past 12 months[5].

**Bottom line:** By focusing on known threats, organizations can build the foundation for a comprehensive cyberdefense.

The mainstreaming of cybercrime makes it difficult for organizations to stay ahead of the bad actors. A robust black market exists on the Dark Web for attack techniques, tools, and stolen data, providing easy access to anyone who wants to wreak havoc on poorly protected systems.

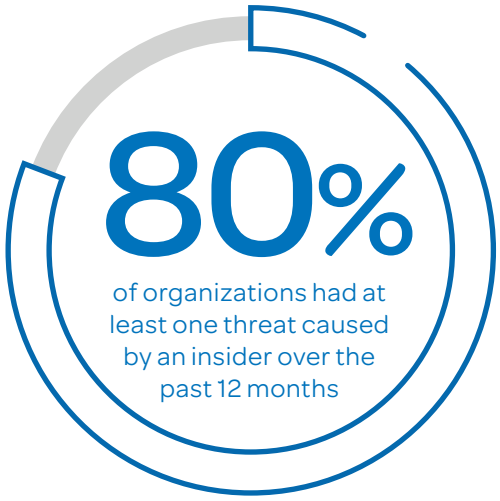
The result is a tsunami of known threats. In the United Kingdom, cyber-enabled fraud and computer misuse surpassed all other crimes in the region in 2015, measured by the number of

incidents and victims[6]. Some experts believe the problem is even worse in the United States, with one estimating that cybercrime in the U.S. is larger than the narcotics trafficking industry[7].

The exclusive AT&T Market Pulse: The Global State of Cybersecurity survey found that 90% of U.S. organizations experienced at least one malware-related incident over the previous 12 months, with 58% acknowledging occasional or frequent malware threats. Nearly three-quarters of respondents reported at least one incident involving unauthorized access to corporate data and at least one denial-of-service (DoS) incident.

These frequent attacks underscore the fact that cybercrime has become a global business. The prevalence of malware attacks was consistent across survey respondents in the U.S., Europe/Middle East (EMEA), and Asia-Pacific (APAC) regions. APAC companies experienced higher rates of unauthorized access to corporate data and DoS attacks than their counterparts in other regions.

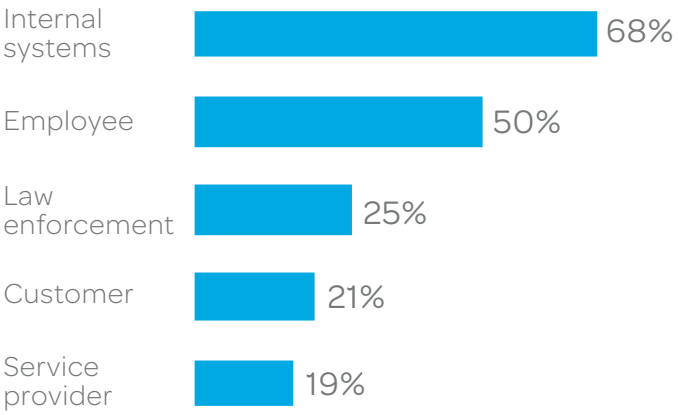
Just as troubling is that existing methods aren't catching all of the successful attacks. In our survey, 25% of organizations that had suffered a data breach were notified of the incident by law enforcement, and 21% were notified by customers. The impact of the worst data breaches all organizations suffered averaged 6 on a 10-point scale where 10 is the most severe. Impacts of successful attacks included downtime (46%), loss of revenue (28%), reputational damage (26%), and loss of customers (22%).




Source: AT&T Market Pulse: Global State of Cybersecurity

### *How data breaches are discovered*

Organizations that suffered a recent data breach were notified by a variety of stakeholders




Source: AT&T Market Pulse: Global State of Cybersecurity

Let's take a look at some of the more widely known, yet persistent threats — and what you can do to help reduce your exposure.

## Malware

We're far removed from the creation of malware in the 1970s as an intellectual exercise by early software coders. Malware evolved further during the 1990s into a prankster's tool for displaying splash screens with scrambled code or laughing skulls. Today it has gone mainstream, with creators selling their products to a broad and eager customer base that ranges from nation states to hacktivists. Luckily, most malware variants are known — meaning the majority of attacks can be blocked with appropriate safeguards in place.

Cybercriminals are certainly taking advantage of this sophisticated tool chest. Members of a Russian cybercriminal gang were arrested

in the spring of 2016, accused of stealing $45 million from banks and other institutions. The gang operated by depositing a sophisticated type of malware called Lurk, first seen in 2011, on legitimate web servers. Once the websites were compromised, anyone visiting the site became infected with the Trojan malware[8].

A growing stockpile of known malware, worms, and viruses is overwhelming organizations. The volume of unsolicited emails with detected malicious attachments increased 300% from the first quarter of 2015 to the same period in 2016[9]. Depending on the day of the week, AT&T intercepts anywhere from a few thousand to more than 2.5 million malicious messages daily. For example, AT&T logged a seven-fold spike in ransomware and information-stealing Trojans over a two-month period in mid-2016. Malicious messages trended upward from approximately 250,000 on July 1 to 1.75 million on Aug. 30.

Malware is like any other software, with developers seeking to continually improve its functionality. As organizations adopt new defensive measures, malware creators respond with their own innovations and then release those new variations for anyone to purchase.

For example, a malware strain called Angler (first seen in 2013) was previously the world's most popular exploit kit, but criminals have recently shifted to Neutrino (discovered in 2013) following a cybercrime bust by Russian authorities. Available on the black market, Neutrino can deliver different payloads to victims based on specific data points such as geolocation, browser platform, and operating system[10].

**300%**

*increase in malicious email attachments from 2015 to 2016*

*"Generally, 25% to 30% of employees still click on suspect links."*

Brian Rexroad
Executive Director
Technology Security
AT&T

Attackers are also evolving their methods by creating malicious macros with complex code to evade traditional malware detection methods. The macros, once enabled by an unsuspecting user, examine a system's list of recently opened files to determine if it is a good target for execution to deliver malware or ransomware.

Malware business models are built on casting a broad net to compromise as many computers as possible. That makes every organization a potential malware target, though smaller businesses with limited IT and cybersecurity resources are more susceptible to a successful attack.

Some of the most common pathways for malware payloads rely on poor security practices among employees, vendors, or contractors who are authorized to access internal systems. Eighty percent of organizations in our survey experienced at least one threat over the past 12 months that was attributed to an insider. These insiders may have an axe to grind, but more likely they unwittingly exposed a digital door to malicious code by opening an infected email or downloading unauthorized software from the internet.

"Generally, 25% to 30% of employees still click on suspect links," says Brian Rexroad, executive director of Technology Security at AT&T.

# Ransomware

Ransomware has joined the list of known threats, as attacks have soared in the last year[11]. Over the summer, ransomware attacks against AT&T clients were trending above 30%, but dropped significantly in August. Clearly, this threat has developed into a volatile issue over the past year, with organizations of all sizes vulnerable to attack.

A volume-based business, this particularly destructive type of malware targets individual users and organizations with demands for relatively small payments. But those ransoms add up: This form of digital extortion is estimated to become a billion-dollar business in 2016[12].

Historically, cybercriminals have targeted high-value assets such as credit cards, Social Security numbers, and business plans. In comparison, ransomware can take advantage by digitally hijacking assets that may have little value outside of the organization. With ransomware, criminals use malicious code to block access to files, folders, or servers until a fee is paid for a decryption key.

In the AT&T survey, 63% of all U.S., EMEA, and APAC organizations were confronted with at least one ransomware incident over the past 12 months. Large U.S. enterprises with 5,000 or more employees were three times as likely as smaller organizations to be subject to ransomware attacks.

While the ransomware concept remains the same as when it first appeared on a floppy disk in the late 1980s, a variety of ransomware programs have been mainstreamed, with new or updated variants springing up regularly on Dark Web marketplaces. For example, Bart is a ransomware variant that targets business-related document formats, personal files including images and videos, and software source code files for encryption. Bart adds the files to a password-protected ZIP archive, making it easier to encrypt files on victims' computers[13].


Source: AT&T Market Pulse: Global State of Cybersecurity

In addition, the ransomware Locky evolved yet again over the summer to make it even more difficult to detect[14]. Given that Locky is often delivered in socially engineered emails containing malicious ZIP attachments, improved spam-blocking techniques reduce the likelihood that it can breach your defenses. As with many known ransomware variants, restricting administrative privileges on computers acts an effective deterrent while regularly backing up data allows recovery if the ransomware is able to evade your malware detection tools.

# Advanced Persistent Threats (APTs)

Attackers' ability to operate in stealth mode is becoming commonplace — and should serve as a wake-up call to security teams. The disclosure by the Democratic National Committee (DNC) in June 2016 that attackers had operated for months, undetected, within their computer systems injected a troubling twist into the U.S. presidential election. The attackers — reported to be two known Russian espionage groups — allegedly tunneled into the DNC's systems using a spear phishing technique, stealing emails, opposition

research, and donor information[15]. It was the latest chilling example of an APT, and it begs the question: What cyberthreats are lurking in your organization?

"I think most security people would admit that if a motivated APT actor wants to get a foothold in your company, they will be able to do so eventually," says John Hogoboom, technical staff lead for the Chief Security Organization at AT&T. "The hope is to be able to detect APTs rapidly through threat analysis and to minimize their persistence and impact to business." Sectors that AT&T frequently sees targeted include government agencies, aerospace and defense, telecommunications, energy, electronics, law, international policy, and humanitarian organizations.

In our survey, 65% of respondents in the financial services sector experienced more than one APT-related issue, followed by technology companies (69%). On a regional level, 69% of U.S., 66% of EMEA, and 70% of APAC organizations had an APT attack in the past 12 months.

APTs are among the most sophisticated forms of cyberattacks, with the ability to run undetected for weeks, months, or even years. The earliest APT attacks — dating back decades — targeted military and defense contractors. U.S. businesses became aware of APTs within the past 10 years or so, when some countries began using them to steal intellectual property.

Today, many APT attacks may still be traced to nation states engaging in cyberespionage or — more recently — political mischief. In addition, cybercriminals have adopted APT techniques to steal money, credit card data, or intellectual property. For this reason, while the defense industry remains a prime target, organizations in any industry must be wary of the APT threat. Cybercriminals are also increasingly repurposing off-the-shelf malware rather than building their own[16], a further indication that APTs are becoming more mainstream.

APT attackers breach an organization's defenses with malware, stolen credentials, or some other means. Once inside, the attackers lie low and avoid detection as they move throughout the network. Their aim: discovery of servers with

## Know the term:

### *APT (Advanced Persistent Threat)*

A targeted attack that penetrates a network without detection and maintains access for a period of time, all while monitoring information or stealing resources. APTs may continue for years

### *Defending against APTs: A multilayered approach*

| *APT stage* | *Defense — containment — mitigation* |
|---|---|
| Initial breach | Stay current with patching to limit known vulnerabilities. Security controls such as firewalls, malware scanning, employee education, and other protections can help to reduce the likelihood of a successful penetration. |
| Internal network reconnaissance and access | Security information and event management (SIEM) systems, threat analytics, and behavioral analytics solutions can analyze log data to help identify abnormal traffic and user activity. |
| Data theft | Data loss prevention and other tools can identify theft attempts. Machine-learning algorithms can help to identify unusual traffic volumes sent to suspicious destinations. Should data theft occur, strong desktop and server backup policies will help to recover from a disruptive attack. |

valuable information, followed by theft of the data. APTs can become even more elusive when they install a second piece of malware that can continue the attack if the initial intrusion is detected.

Unlike other types of cyberbreaches, which demand immediate counteractions, APTs require a different type of action to block their possibly devastating effects. Once detected, quietly determining the extent of the APT before taking steps to eradicate it may help in foiling the successful launch of a second malware payload. “Don’t let them know that you know,” says Hogoboom.

## Distributed Denial of Service (DDoS)

The first documented denial-of-service attack over the internet occurred in February 2000, when a 15-year-old Canadian hacker launched a series of strikes against Amazon, eBay, and other e-commerce sites[17]. This was the dawn of DDoS, in which attackers enlist dozens, hundreds, or thousands of compromised machines — collectively to overwhelm the websites of targeted victims with traffic.

DDoS attacks have since become common, with 73% of global survey respondents reporting at least one DDoS-related issue in the past year.

**15%**

*APAC organizations were 15% more likely than U.S. organizations to have had a DDoS attack in the past 12 months.*

Source: AT&T Market Pulse: Global State of Cybersecurity

# What does DDoS extortion look like?

The prospect of having your digital assets held hostage can strike panic at almost every level of an organization — from IT administrators and managers to executives and board members. Digital extortion can take many forms, including ransomware and DDoS attacks that block access to websites. In addition to a strict payment timetable, cyberattackers using one of these methods often insist on payment in bitcoins — a form of digital currency — for the anonymity of everyone involved in the transaction. Bitcoin's value can fluctuate greatly; as of September 1, its value was $571.

How are these demands delivered? Here's an excerpt from an actual email received by an organization that wishes to remain anonymous.


"Please forward this email to someone in your company who is allowed to make important decisions!

We have chosen your company as a target for our next DDoS attack.

All of your servers will be subject to a DDoS attack starting Friday.

Right now we are running a small 1 hour demo attack to prove that this is not a hoax.

What does this mean? This means that your website and other connected services will be unavailable for everyone; during the downtime, you will not be able to generate any sales. Please also note that this will severely damage your reputation among your users / customers as well as strongly hurt your Google rankings (worst case = your website will get de-indexed).

How do I stop this? We are willing to refrain from attacking your servers for a small fee. The current fee is 15 Bitcoins (BTC). The fee will increase by 15 Bitcoins for each day that has passed without payment.

What if I don't pay? If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution. We will completely destroy your reputation among Google and your customers and make sure your website will remain offline until you pay.

Do not reply to this email — don't try to reason or negotiate — we will not read any replies. Once you have paid we won't start the attack, and you will never hear from us again!

Please note that Bitcoin is anonymous, and no one will find out that you have complied."

## *Epilogue*

The story of this extortion attempt had a happy ending. By teaming up with AT&T services, the organization was prepared for just such an attack and able to completely block the effects of the attacker's threats.


Compared to respondents in the U.S., those in APAC were 15% more likely to have been attacked. But in all regions, there seems to be little slowdown in the number of DDoS attacks. Since 2013, AT&T has logged constant DDoS attack attempts on its clients (see "What does DDoS extortion look like?").

This proliferation is due, in part, to the relative ease of launching DDoS attacks. Hackers have published DDoS kits that anyone can download to craft and mount an attack — even high school students who use them to shut down their schools' websites or cripple online operations such as taking attendance, distributing grades, or administering tests[18]. AT&T has logged a 22% increase in DDoS attacks against schools since 2014. For one school district, AT&T recorded 30 attacks for the 2015-2016 school year.

While any type of organization can fall victim to these attacks, those engaged in divisive industries or activities, ranging from genetic engineering to politics, are perennial targets of hacktivist groups. In the financial services sector, for example, 82% of respondents in the AT&T survey have experienced at least one incident, with 47% experiencing multiple attacks. Since 2013, the financial sector has accounted for 39% of all DDoS attacks mitigated by AT&T.

DDoS attack vectors have evolved as organizations mount defenses against known methods. One increasingly popular technique is to compromise different communications protocols and turn them into amplifiers to multiply the volume of the attack.

## Fighting the knowns

A few high-profile breaches — from ransomware attacks on hospitals to leaked emails from the DNC — obscure the real challenge for most organizations: The vast majority of threats are known, but organizations continue to be vulnerable because of poor practices (see "Preparing for the knowns"). To help protect your organization against mainstream attacks, these components of a multilayered approach are particularly important:

- Consistently back up data and store it offline.
- Conduct employee awareness training focused on the types of emails and other methods that are used to distribute malicious malware.
- Update software with patches as they become available.
- Deploy firewalls and other security solutions across every endpoint to help reduce vulnerabilities.

# What's next: Emerging vulnerabilities

*In this section:*

**IoT:** AT&T has recorded a 3,198% increase in IoT vulnerability scans over the past three years.

**Cloud:** Companies with more than 50% of their data in the cloud report higher attack rates[19].

**Mobile:** 40% of organizations have had their employees' mobile devices compromised in the past 12 months[20].

**Bottom line:** As known threats expand to new platforms, organizations should recognize the distinctive risks of emerging technology while remaining true to foundational security practices.

The scope of known threats is increasing dramatically as organizations become more digital across internal and customer-facing operations. In particular, rapid adoption of the Internet of Things, cloud technology, and mobile devices, while providing significant benefits to organizations, has also given rise to increased levels of cybercriminal activity.

How do you deal with these ever-mutating threats? It comes down to recognizing the unique security demands of each new technology in your cybersecurity practices.

# Internet of Things

About 6.4 billion connected "things" — from car sensors to pacemakers — are expected to be online worldwide in 2016, up 30% from a year earlier[21]. Respondents to the AT&T survey have an average of just over 1,500 connected devices in their organizations.

IoT deployments are expanding as organizations connect previously siloed applications. Obvious integration points are smart cities and smart cars. In Songdo, South Korea, cars equipped with radio frequency identification (RFID) tags automatically transmit data to municipal systems that analyze the information for transportation planning — and share the results with residents. In the U.K., Jaguar is working with local agencies to send real-time data about road hazards — culled from its in-vehicle platform — to municipal road crews[22].

Expansion in the scope of our increasingly interconnected world brings heightened concerns about security threats. Over the last three years, AT&T has recorded a 3,198% increase in IoT vulnerability scans. The research firm IDC predicts that by 2018, approximately two-thirds of enterprises will experience some sort of IoT security breach[23]. It's simple, really: More IoT deployments create more possible points that hackers can exploit.


Source: AT&T Market Pulse: Global State of Cybersecurity

Fifty-eight percent of U.S.-based respondents to the AT&T survey don't have confidence in the security of their own connected devices, compared with 35% of respondents in EMEA and 29% of those in APAC.

Those confidence levels may dip in coming years. As more devices are connected, the risk of a major breach increases, particularly as organizations bring more device makers, developers, vendors, business partners, and even customers into their IoT ecosystems.

## Securing devices from known threats

Given how IoT data often flows well beyond an organization's traditional defenses, vulnerabilities increase when your data is exposed to third-party devices and systems with less stringent controls[24].

Part of the challenge comes back to the unique nature of IoT deployments.

"Traditional security doesn't meet all of IoT's security needs," says Chris Penrose, senior vice president for Internet of Things Solutions at AT&T. "Unfortunately not all users think about new security risks and simply follow the security practices that they have always used."

Safeguarding your organization's IoT devices requires a proactive, multilayered approach that's tightly aligned with your overarching cybersecurity strategy. Risk assessments of your own IoT devices and policies, as well as those of your third-party vendors, should be folded into your overall risk profile. Only then can you know — and manage — all of the points where your data and devices are potentially under threat.

# Cloud technology

More than 90% of companies are estimated to already use some form of cloud technology in their operations as they look to scale projects

in more cost-effective and nimble ways[25]. By the end of this decade, over one-third of all data will reside in or pass through the cloud[26]. Companies in the AT&T survey have moved, on average, 33% of their data to the public cloud.

More and more, IT professionals consider cloud platforms to be equally or more secure than on-premises systems[27]. About six in 10 companies in the AT&T survey show high levels of confidence that their data residing in the public cloud will be secure for the next 12 months.

Are leadership teams right to feel so confident? The vast amount of data stored in the cloud is an appealing target for known threats. In the AT&T survey, companies storing more than half of their data in the cloud report a higher frequency of malware, ransomware, APTs, theft of proprietary information, and unauthorized access to corporate data than those that store less than half of their data in the cloud. It's wrong, however, to assume that data is most vulnerable when it's in the public cloud and safest when it's locked away in the corporate data center.

"You can't put sandbags around an organization's perimeter anymore. Security now must rely on virtual firewall capabilities," says Andy Daudelin, vice president for Cloud and Cloud Networking at AT&T.

## Know the terms:

### *Man-in-the-middle*

An attacker who secretly intercepts and possibly modifies messages between two parties

### *Zero-day attack*

A new type of cyberattack that hasn't been seen before

# Profiling cyberattacks

Over the past two years, high-profile flaws in the most widely deployed security protocol, SSL, have come to light, creating avenues for new attack types. But the steps needed to avoid such attacks — patching and configuration changes — are also widely known and easily available.

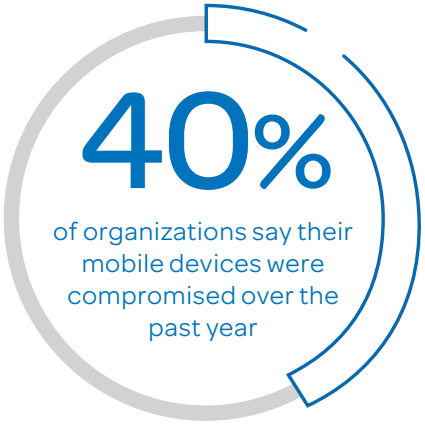
According to Digital Defense Inc., the most prevalent, high-profile threats resulting from protocol weaknesses affect cloud-hosting and perimeter systems. For example:

**Poodle** takes advantage of a flaw that makes it easier for man-in-the-middle attackers to steal data. This flaw continues to be one of the most widely unpatched vulnerabilities on the internet, say DDI experts.

**Drown** allows attackers to break an organization's encryption codes to steal sensitive information, including passwords, credit card numbers, trade secrets, and financial data. Similar to Poodle, it relies on a man-in-the-middle attack.

**Cipher Zero Authentication Bypass Vulnerability** can allow an attacker to take control of operating system software and access the system through a flaw in the IPMI protocol.

Companies typically can help address these flaws by sweeping systems for the vulnerabilities and then applying vendor-supplied patches or the appropriate configuration changes.




Source: AT&T Market Pulse: Global State of Cybersecurity

## Defending your cloud against known threats

Questions surrounding cloud security often mirror those for enterprise security in general. Attackers are using many of the same basic techniques to break into cloud-based services that they have employed for years — including social engineering and DDoS attacks.

For example, a phishing campaign left users of Microsoft's cloud-based Office 365 software exposed to a potentially massive ransomware attack. The attackers sent emails to millions of Office 365 users infected with a strain of the Cerber ransomware. Clicking on the email's attachment would have triggered a macro that encrypted a user's files along with an audio demand for ransom. Fortunately, Microsoft responded quickly and was able to block the malware a day later[28].

But the security of a cloud service provider shouldn't be your only concern. Focusing on the link between the cloud and your organization is just as key to protecting your network. With services such as MPLS VPNs, the security risks of cloud technology are reduced by securing your internet connection.

Cloud security also can be jeopardized when IT teams don't have control over who purchases cloud services across the organization. The "as-a-service" model has made it easy for any employee to purchase a cloud product — whether it's a personal application such as Dropbox or a department-wide service such as Salesforce. IT may not even be aware that these applications exist, and without proper governance, unauthorized applications may be vulnerable to weak security controls that attackers can exploit.

This growing challenge has prompted more organizations to use cloud access security brokers. CASBs act as gatekeepers for cloud-based services in use across the organization (see "A more secure approach to the cloud").

# Mobile devices

Although the majority of cybersecurity professionals in the AT&T survey express confidence in the security of employees' work-related mobile devices, about 40% admit that their mobile devices had been compromised occasionally (26%) or frequently (11%) over the past 12 months. The correlation between confidence level and security incidents is an awkward fit, to say the least.

The challenge is growing. As malicious code writers target mobile devices in greater numbers[29], cybercriminals are embedding malware into legitimate applications. Attackers are increasingly targeting app stores to distribute mobile apps loaded with malware — including wildly popular apps such as Pokémon Go. It took just 48 hours after the release of Pokémon Go in 2016 for hackers to create a repackaged, malware-laden version of the app for distribution on third-party app stores and internet file-sharing sites[30].

The challenges extend beyond apps. Wi-Fi hot spots that aren't under the control of your network administrators continue to pose risks to enterprise data. Negligent or naïve employees are weak links in the enterprise security chain. Connecting to free public

## Know the term:

### *BYOD*

Bring-your-own-device is a business practice of permitting employees to use their own devices — computers, smartphones, tablets, or other devices — for work

Wi-Fi at a coffee shop or the airport is done without regard to the potential consequences of exposing corporate assets to man-in-the-middle attacks that grab every piece of data — including email and app content — sent over the unsecured site.

What's more, scammers who set up rogue Wi-Fi access points can mimic the characteristics of a trusted network. Users are fooled into connecting to their access point, where the criminals can steal personal data and passwords that provide access to corporate systems.

The bring-your-own-device (BYOD) trend adds to the challenges of mobile security. Increasingly, employees are using their personal devices for work — accessing enterprise systems while on the road and at home. But they're also using those mobile devices for personal tasks. Delivery drivers use company-approved smartphones to track deliveries — but then casually surf the internet during downtime. Digital-savvy employees use their work phones to purchase goods at smart vending machines that can be compromised by an adept hacker.

At the enterprise level, the lack of robust, end-to-end encryption — for data that is stored and in transit — can spell disaster. Consider the possible consequences of the theft of an employee's unencrypted laptop: The personal records of thousands of customers are exposed and the organization is brought to a complete stop while reacting to the breach.

## Locking down your organization's portable devices

Security challenges can vex enterprise security managers as they strive to deliver a highly secure mobile environment while being sensitive to users' experience. Issuing corporate edicts that prohibit employees connecting to unsecured Wi-Fi, for example, may be tempting but is unlikely to eradicate the problem. One way to address the challenge is coming into focus: Mobile device security should be integrated into an organization's overall cybersecurity strategy.

# A more secure approach to the cloud

Cloud-computing services used without explicit organizational approval hold the potential to introduce a host of new cybersecurity risks. CIOs and CSOs agree that cloud services provisioned without IT's knowledge represent the greatest security risk[31].

Enter the cloud access security broker (CASB), a third-party entity that enforces security policies tailored to an organization's specific needs, industry and regulatory requirements, and access policies. When paired with a cloud broker — which helps organizations provision and manage cloud services — CASBs keep a watchful eye on cloud applications and data.

CASBs perform basic tasks, such as logging security threats and anomalies and providing the necessary alerts and recommended responses to security teams. They may also provide additional controls such as time-of-day restrictions or blocking users in certain locations or on certain devices from accessing services.

CASBs can help IT and security teams keep cloud-based services as highly secure as the on-premise systems that they control directly.

# Priorities for the year ahead

*In this section:*

**Risk assessments:** A risk assessment will help your organization set priorities for cybersecurity investments.

**Automation tools:** Organizations have a growing arsenal of tools to help mount strong defenses against known threats.

**Awareness & training:** The ultimate success of a security strategy rests with employees.

**Bottom line:** Defending against known threats requires attention to three core elements: risk assessment, tools, and training.

No doubt, organizations face a daunting set of challenges from known threats and the mainstreaming of cyberattack tools and methods. Overcoming these challenges requires attention to three core components: risk assessment, tools, and training.

## Risk and vulnerability assessments

Whether a large multinational corporation or a medium-sized store chain, all organizations can benefit from adopting a two-phase methodology for assessing their risk:

**Information gathering.** Phase one sets the scope for the risk assessment and documents relevant systems, networks, and a variety of operational processes. This phase also spots possible threats and vulnerabilities.

**Risk analysis.** Phase two involves a control and impact analysis of the collected information to evaluate the likelihood of a breach. Organizations learn the overall risk of a cyberthreat attacking a given vulnerability within their system.

The outcome of the analysis depends on an organization's size, industry, and goals. For example, some options for mitigating risk — such as preparing for a zero-day attack — may only make business sense for large banks or multinational corporations.

## Aligning resources with weak spots

Your investments should align with identified weak spots. But cybersecurity investments involve more than preventive tools, of course. Organizations that make security a priority invest in a multilayered approach that encompasses:

**Prevention.** 89% of organizations in the AT&T survey will invest in intrusion detection and prevention initiatives over the next year.

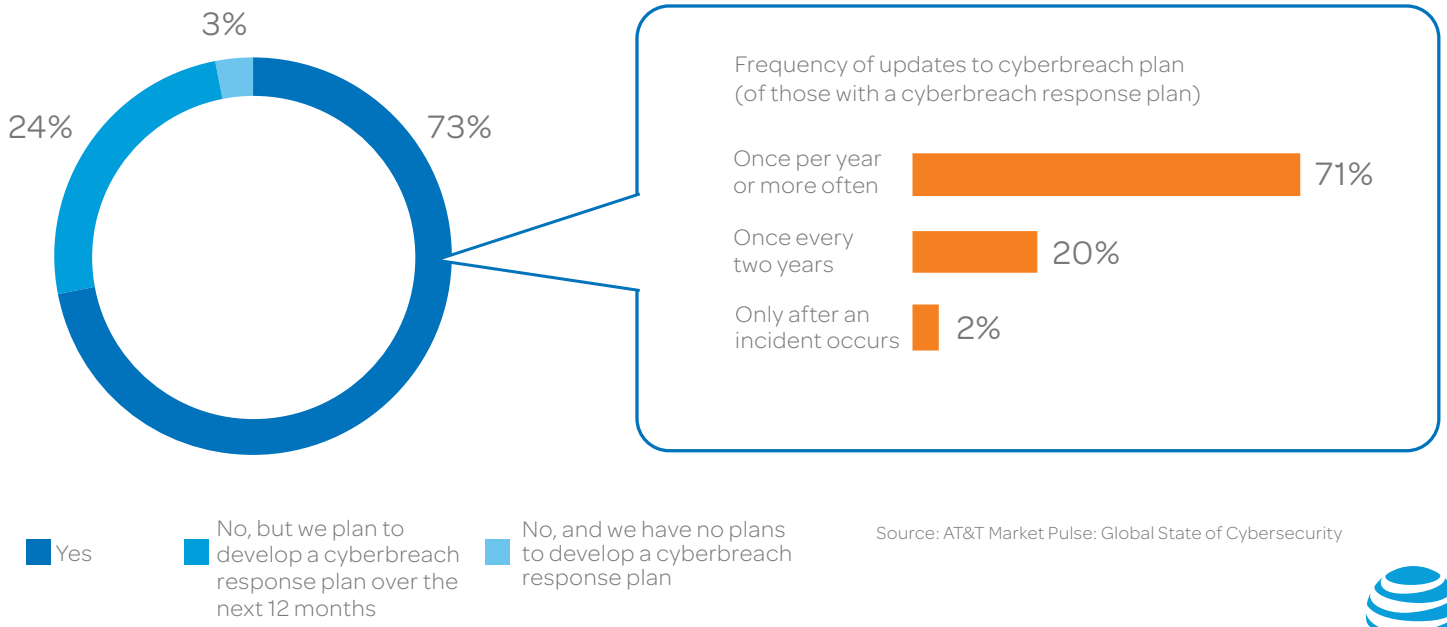
**Threat detection.** More than 8 in 10 organizations are investing in tools for threat monitoring, threat analysis, and mitigation.

**Incident response.** 85% of organizations plan to continue or begin investing in an incident response program. But as was discussed in our previous Cybersecurity Insights report, simply having an incident response program isn't adequate. Frequent testing is required to help your organization respond swiftly and effectively to a breach.

Cybersecurity insurance is another area for consideration. A robust 89% of survey respondents either have a cybersecurity insurance policy in place or plan to purchase one — a further hedge to help against the impact of both known and unknown threats. As risks grow in volume and scope, insurance premiums are expected to triple to $7.5 billion by the end of the decade, from around $2.5 billion today[32] (see "Cyberinsurance: A new frontier").

### *A growing emphasis on incident response*

Do you have a cyberbreach response plan?




Source: AT&T Market Pulse: Global State of Cybersecurity


# Cyberinsurance: A new frontier

With breaches happening all too frequently, insurance policies specifically designed to cover cyberrisk have become more appealing. More than 50 insurance companies now offer cybercoverage, according to the Financial Services Roundtable[33]. But in an evolving market, no two policies are alike, and that can make buying cyberinsurance a somewhat difficult proposition.

In this new market, costs of a data breach can vary widely depending upon the type of data stolen, the industry, and company size. Emerging threats can also make it difficult to determine adequate coverage. Two years ago, few people had even heard of ransomware. It's one of the fastest-growing categories of cybercrime, but few policies cover it.

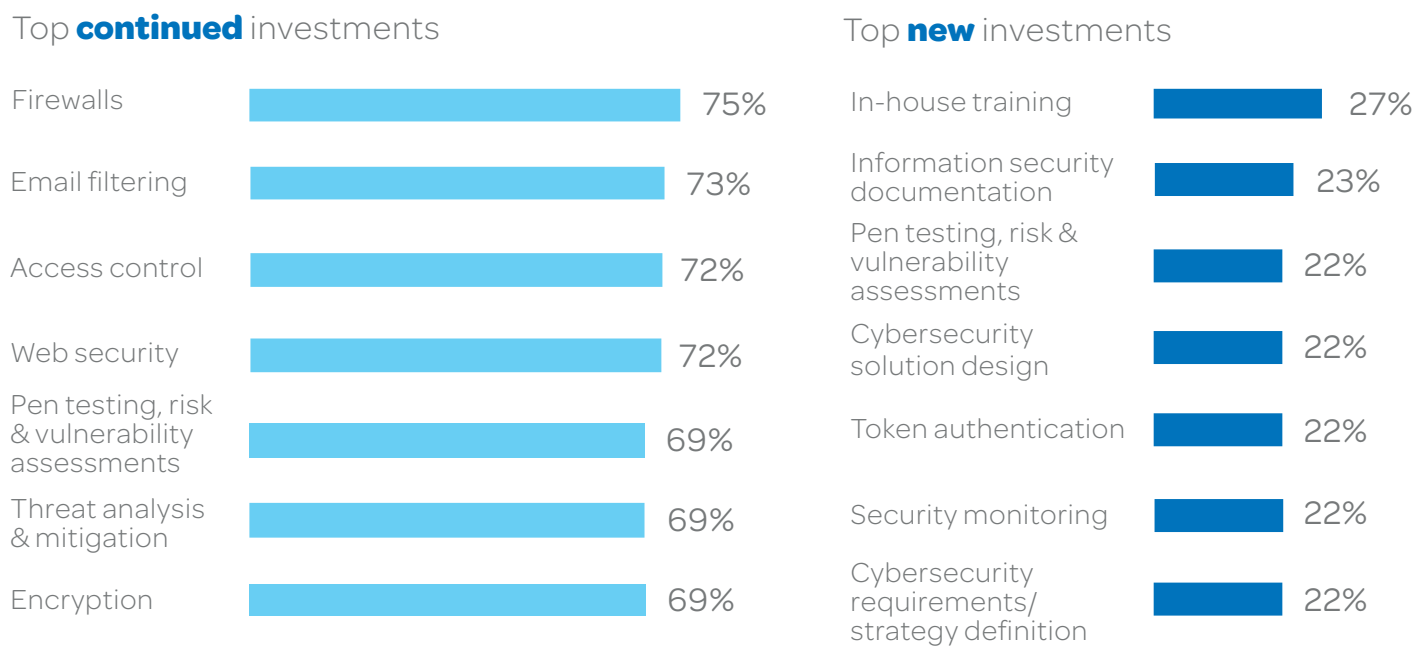
There is no "one size fits all" policy. Prospective buyers should consider their industry, products and services, data risks and exposures, the quality of existing IT security, and revenues.

Other factors to consider before purchasing cyberinsurance include your organization's vulnerability and potential losses, the cost of notifying compromised individuals, identity theft protection, regulatory penalties, loss of market value, brand damage, legal fees, technology fixes, and management time lost dealing with the problem.

Policy exclusions also can vary. For example, some insurers won't pay for select legal fees or for damage to the organization caused by a state-sponsored attack.

Nearly all insurers require sound security practices from their policy holders. Failure to use strong access controls, encryption, password protection, and even formal employee education, among other measures, can result in a denial of coverage.

## *Investment plans for the next 12 months show a mix of traditional defense, training, and advanced tools*




Source: AT&T Market Pulse: Global State of Cybersecurity

## Tools: A shift toward automation

A new generation of threat analytics tools is helping overwhelmed security analysts identify the most serious threats lurking amidst the alert noise. But their greatest strength may be their ability to counter those threats with little or no human intervention. More than half (56%) of survey respondents plan to increase their investment in next-generation tools such as threat analytics and machine learning technology over the next three years.

The application of big data analytics to threat identification and mitigation has quickly emerged as one of the more obvious uses of this technology. Not only are the volumes of cybersecurity data staggering, so are the time demands associated with them. Even a brief delay in identifying a threat can mean the difference between neutralizing an attack and falling victim to a breach.

*"We now can combat attackers by helping machines learn faster than attackers can invent."*

Chris Parsons
Vice President
Big Data Strategy & Business Development
AT&T

Big data analytics takes the problem of too much data and turns it on its head — the more data these systems have to work with, the more effective they can be. Adding machine learning to the mix can increase insights further by teaching systems to identify new cyberthreats on their own and alert their human partners.

"We now can combat attackers by helping machines learn faster than attackers can invent," says Chris Parsons, vice president for Big Data Strategy and Business Development at AT&T.

# *Preparing for the knowns*

## How to help protect your organization against the majority of cyberattacks

### Harness technology

Most breaches result from common malwares, viruses, and worms, meaning technology exists for detecting and preventing their intrusion into your organization. Use this checklist to help stop the bad actors before they stop you.

*1. Risk assessment*

*2. Data loss prevention*

*3. Protected networks*

*4. Email filtering*

*5. Web application firewall*

*6. Threat monitoring*

*7. Incident response*

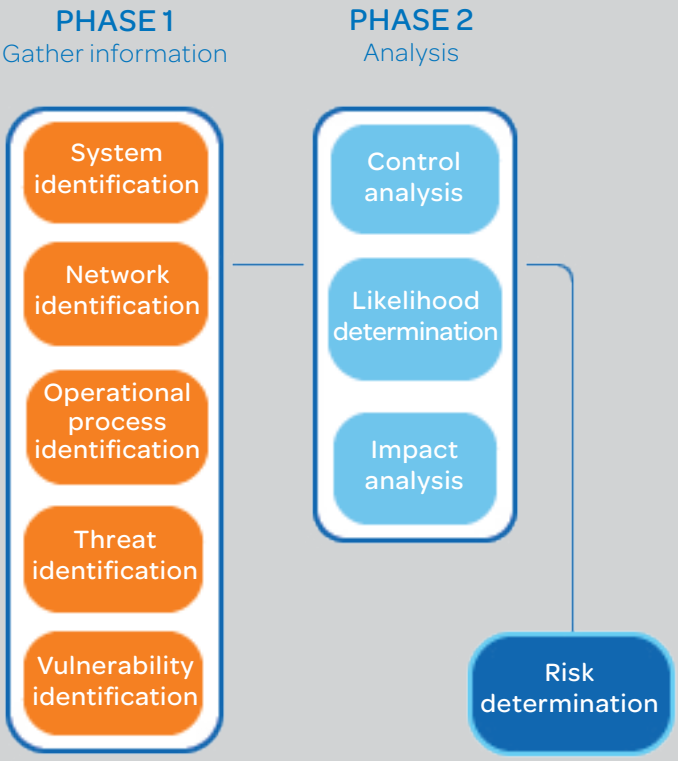
*8. DDoS*

*9. Encryption*

*10. Identity management*

### Conduct a risk assessment

Pinpoint your weaknesses and know the likelihood of a successful attack anywhere in your organization.




# Awareness and training: Not one and done

A simple click on an email link is all it takes to leave an entire company vulnerable to a devastating attack. By engendering a culture of cyberawareness and responsibility among employees, an organization can significantly strengthen its cybersecurity posture.

Not investing in cybersecurity awareness can have severe consequences:

- Losses resulting from employee negligence are growing, with no slowdown in sight. More than 7,000 businesses in the U.S. suffered accumulated losses of around $740 million after their employees fell for email-based phishing scams between 2013 and 2015[34].

- In 2016, cybercriminals modified an old phishing scam that targets company payroll departments, fooling them into providing W-2 tax forms containing Social Security numbers and other personally identifiable information[35].

- Employees continue to ignore warnings not to plug USB flash drives from unknown sources into their computers. When researchers from the trade association CompTIA ran an experiment leaving the storage devices in public locations in Chicago, Cleveland, San Francisco and Washington, D.C., about 20% of the people who found the flash drives plugged them into their own devices[36].

A cyberaware company recognizes that employee education requires more than office posters and reminder emails. In the AT&T survey, 27% of organizations are planning new in-house training investments over the next 12 months. However, almost 10% have no budget set aside for security awareness training.

"Targeted education goes a long way in employee compliance with security policies,"

says Sundhar Annamalai, executive director for Integrated Solutions at AT&T.

Employees need to understand that threats aren't limited to phishing emails. They include phone calls from cybercriminals posing as help desk representatives; or free tablet offers to employees who register with work-related information; or unsecured or fraudulent Wi-Fi hotspots; or weak passwords used for personal and work login credentials. Training should expose employees to the broad spectrum of threats — along with tips on the role everyone plays in their mitigation.

Such tactics are scalable for any budget; campaigns can launch with a few short videos or an infographic. At a minimum, you want employees to leave with an appreciation of cybersecurity basics: how cybercriminals can use social engineering to gain their trust and infiltrate your organization.

*"Targeted education goes a long way in employee compliance with security policies."*

Sundhar Annamalai
Executive Director
Integrated Solutions
AT&T

# Conclusion: Your call to action

Detecting and responding to threats isn't getting easier. A rising tide of known threats and the mainstreaming of cybercriminal activities have created an undercurrent of concern: Are we doing enough to defend against known threats? Where will the next threat come from?

The sheer volume of attacks detected by AT&T defenses each day is enough to give pause to any leadership team. But it's important to remember what we told you at the beginning of our report: More than 90% of cyberattacks are known threats and, therefore, steps can be taken to help detect and prevent them by employing the right defensive measures.

Zero-day attacks are the ones that make headlines, but compared to the zettabytes of traffic flowing through countless networks each day, they are relatively uncommon. For cybersecurity and network professionals, it's the common viruses, worms, and their variants that invade relentlessly. The lesson here: Never let down your core defenses.

Persistent execution to counter the known threats that pose the greatest risk will help protect your business from intruders. Keep these core principles in mind:

**Invest in a multilayered approach.** A cyberaware organization effectively balances prevention, threat detection, and response to address the vast majority of known threats. This approach should also tightly integrate all aspects of your digital infrastructure — networks, systems, cloud-based services, and endpoint devices ranging from desktops to smartphones to smart devices connected via the IoT.

**Reduce impacts from your weak links — employees and vendors.** Employees and third-party vendors may not share your urgency or your diligence around good cybersecurity practices. Awareness and education programs are instrumental for your workforce to take accountability for their security. For contractors, business partners and vendors, clearly articulated policies and controls should be a requirement.

**Keep your patches and software applications current.** While most threats are known — with security protections available to help stop their attack — their variants can still threaten your organization. Keeping current on software patches and updates will help your organization avoid the dangers of software vulnerabilities.

**Make cybersecurity foundational.** Many organizations are undergoing comprehensive IT transformation efforts that involve moving to more flexible infrastructures utilizing cloud services and software-defined systems and networks. Make sure that security is a foundational component of these initiatives, so that your organization is positioned to be more agile and highly secure.

Adversaries are always looking for the next way into your organization. Your cybersecurity practices must be just as determined to keep them out.

# Additional reading




- Cybersecurity Insights, vol. 1: What Every CEO Needs to Know About Cybersecurity
  business.att.com/cybersecurity/archives/v1
- Cybersecurity Insights, vol. 2: The CEO's Guide to Securing the Internet of Things
  business.att.com/cybersecurity/archives/v2
- Cybersecurity Insights, vol. 3: The CEO's Guide to Cyberbreach Response
  business.att.com/cybersecurity/archives/v3
- Executive Abstracts
  business.att.com/cybersecurity/abstracts
- Know the Terms glossary
  business.att.com/cybersecurity/terms
- Network Security Solutions
  business.att.com/enterprise/portfolio/networksecurity
- More resources available at
  securityresourcecenter.att.com

## *About our survey*

To gain a better understanding of the current global state of cybersecurity in large businesses and the current thinking behind security issues, AT&T commissioned a survey of business and IT decision-makers in July 2016. Respondents to the AT&T Market Pulse: Global State of Cybersecurity survey had to be director-level or above at companies with at least 1,000 employees. The self-administered survey returned more than 700 responses globally, covering a mix of functional areas and roles within the organization.

# Endnotes and sources


1. Fitzpatrick, D. and Griffin, D. (2016, April 15), Cyber-extortion losses skyrocket, says FBI. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
2. Kaspersky Lab assists in Russia's largest cybercriminal arrest: The hackers who stole $45 million. http://www.kaspersky.com
3. AT&T. (2016). Market Pulse: The Global State of Cybersecurity
4. ibid
5. ibid
6. National Crime Agency. (July 2016). Cyber Crime Assessment 2016. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
7. Yasin, R. (2016, Aug. 7). Cybercrime now surpasses traditional crime in UK. http://www.darkreading.com/threat-intelligence/cybercrime-now-surpasses-traditional-crime-in-uk/d/d-id/1326208
8. Kaspersky Lab assists in Russia's largest cybercriminal arrest: The hackers who stole $45 million. http://www.kaspersky.com
9. Gudkova, D., et. al., (2016, May 12). Spam and phishing in Q1 2016. https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/
10. Rocha, L. (2015). Neutrino Exploit Kit Analysis and Threat Indicators. SANS Institute. https://www.sans.org/reading-room/whitepapers/detection/neutrino-exploit-kit-analysis-threat-indicators-36892
11. Crypto-ransomware attacks rise five-fold to hit 718 thousand users in one year. (2016, June 22). http://www.kaspersky.com
12. Fitzpatrick, D. and Griffin, D.
13. Constantin, L. (2016, June 27). Bart ransomware shows it can be effective without sophisticated encryption. PCWorld. http://www.pcworld.com/article/3088581/security/bart-ransomware-shows-it-can-be-effective-without-sophisticated-encryption.html
14. Olenick, D. (2016, Aug. 26). Latest Locky version on the loose. SC Magazine. http://www.scmagazine.com/latest-locky-version-on-the-loose/article/518820/
15. Fisher, M. (2016, July 26). Why security experts think Russia was behind the D.N.C. breach. The New York Times. http://www.nytimes.com/2016/07/27/world/europe/russia-dnc-hack-emails.html
16. The end of the world for APTs as we know them in 2016. (2016, Nov. 17). https://securelist.com/files/2015/11/KSB_2016_Predictions_FINAL.pdf
17. Dennis, M.A. Denial of service attack (DoS attack). https://www.britannica.com/topic/denial-of-service-attack
18. AT&T. (2016). Helping to Secure Education Networks, https://www.corp.att.com/edu/docs/Security_Whitepaper.pdf
19. AT&T. (2016). Market Pulse: The Global State of Cybersecurity
20. ibid
21. Gartner says worldwide IoT security spending to reach $348 million in 2016. (2016, April 25). http://www.gartner.com/newsroom/id/3291817
22. Underwood, M. (2016, May 30). Smart car, meet the smart city. http://www.thedailybeast.com/articles/2016/05/31/smart-car-meet-the-smart-city.html
23. Wong, C. (2015, Nov. 5). IDC's 2016 predictions: IoT headed for huge growth (and security headaches). http://www.itbusiness.ca/news/idcs-2016-predictions-iot-headed-for-huge-growth-and-security-headaches/60954
24. Saif, I., et.al. (2015, July 27). Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age. http://dupress.com/articles/internet-of-things-data-security-and-privacy/
25. As cloud computing barriers fall, new challenges arise for organizations, new Comptia study concludes. (2014, Nov. 3). https://www.comptia.org/about-us/newsroom/press-releases/2014/11/03/as-cloud-computing-barriers-fall-new-challenges-arise-for-organizations-new-comptia-study-concludes
26. Big data universe beginning to explode. (2012). http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode
27. CSA survey finds trust in the cloud increasing. (2016, Feb. 8). http://www.businesscloudnews.com/2016/02/08/csa-survey-finds-trust-in-the-cloud-increasing/
28. Rashid, F. (2016, June 28). Cerber ransomware targets enterprises via Office 365. http://www.infoworld.com/article/3088703/security/cerber-ransomware-targets-enterprises-via-office-365.html
29. Check Point Research reveals threat of mobile malware persists as attacks targeting iOS devices increase. (2016, April). https://www.checkpoint.com/press/2016/check-point-research-reveals-threat-mobile-malware-persists-attacks-targeting-ios-devices-increase/
30. Duckering, B. (2016, July 11). Pokémon Go malware caught by Skycure. https://www.skycure.com/blog/pokemon-go-malware-caught-by-skycure/
31. IDG Enterprise. (2016, Feb. 8). CIO/CSO Partnership Survey 2015. (2016, Feb 8). http://www.idgenterprise.com/resource/research/tech-ciocso-partnership-survey-2015/
32. PWC. (2016 Jan.). Top issues: The promise and pitfalls of cyber insurance. https://www.pwc.com/us/en/insurance/publications/assets/pwc-insurance-top-issues-cyber-insurance.pdf
33. An assessment of cyber insurance. (2015, February). http://fsroundtable.org/cto-corner-assessment-cyber-insurance/
34. Business e-mail compromise an emerging global threat. (2015, August 28). https://www.fbi.gov/news/stories/business-e-mail-compromise/business-e-mail-compromise
35. Ragan, S. (2016, March 24). Phishing attacks targeting W-2 data hit 41 organizations in Q1 2016. http://www.csoonline.com/article/3048263/security/phishing-attacks-targeting-w-2-data-hit-41-organizations-in-q1-2016.html
36. Find a flash drive, pick it up: experiment shows how lack of cybersecurity knowledge can impact organizations. (2015, Oct. 26). https://www.comptia.org/about-us/newsroom/press-releases/2015/10/26/find-a-flash-drive-pick-it-up-experiment-shows-how-lack-of-cybersecurity-knowledge-can-impact-organizations

*"The majority of cybersecurity threats are known. Defending against the known is a balanced, level-headed approach that better secures your organization."*

Jason Porter
Vice President
Security Solutions
AT&T

MOBILIZING
**YOUR**
WORLD℠

*att.com/cybersecurity-insights*