The CEO's Guide to Data Security

Protect your data through innovation

AT&T Cybersecurity Insights | Volume 5

MOBILIZING YOUR WORLD℠

"Cybercrime damages are expected to rise to $6 trillion annually by 2021[1]. This represents the greatest transfer of economic wealth in history and risks the incentives for innovation and investment."

Karthik Swarnam
Vice President
Security Architecture
AT&T

Contents

For more information:

Follow us on Twitter @attbusiness

Visit us at att.com/security

Executive summary

Innovation is essential to your organization's success and central to your ability to sustain competitive advantage. In our digitally driven world, data has become the lifeblood of innovation.

Data gives organizations better insights that lead to unique products, more efficient operations, superior customer experience, and many other quantifiable benefits. But there's a risk inherent to data-driven innovation. Any advantage you gain can be quickly compromised by cybercriminals.

Face it: Cybercriminals value innovation as much as you. These bad actors are constantly looking for new ways to tunnel into your network or disrupt your business.

Mobile and IoT: More innovation, more threats

As mobile devices become commonplace in most organizations, cybercriminals are exploiting poorly secured smartphones, mobile apps, and unauthorized wireless networks to gain access to sensitive data. Employees may unwittingly download malware-laden mobile apps from unauthorized app stores, opening up new attack vectors. Nearly a third of mobile devices are at medium-to-high risk of exposing enterprise data[2].

In addition, the growth of the Internet of Things (IoT) has pushed the scale and sophistication of cybercriminal efforts to unprecedented levels. Commandeering 100,000 IoT devices for a Distributed Denial of Service (DDoS) attack is no longer theoretical; it's the latest indication that cybercrime innovation is thriving.

Best practices

To reduce risk in this increasingly dynamic environment, your approach to cybersecurity must continuously evolve above and beyond the foundational practices you already have in place.

Cybersecurity innovation means keeping pace with cybercriminals by continually adapting and evolving your organization's security controls and practices for protecting enterprise data. Whether your data resides on an IoT device, a smartphone, a server behind the corporate firewall, or is in transit to or from the cloud, innovation is the new cybersecurity mandate.

A proactive approach to cybersecurity involves securing all components of the digital ecosystem — data, connected devices, applications, networks, and the data center — with the help of innovative technologies and methods that improve how you identify and respond to just not today's threats, but tomorrow's as well (see box).

Importantly, cybersecurity innovation also requires trusted alliances and integration into the broad and growing cybersecurity ecosystem. By relying on security providers, you can adopt and customize products and processes to stay ahead of the bad actors. In today's environment, you can't fight organized cybergangs and nation states on your own.

Innovation has always been a driving force behind business success. At AT&T, we believe cybersecurity innovation is essential to sustained success.

Block evolving threats with innovative technologies

- **Identity & access management:** Authorize access policies for applications, devices and people
- **Threat analytics:** Automate processes for identifying and responding to abnormal activity
- **Virtualization:** Improve flexibility and consistency with software-defined security
- **Incident response:** Institute a playbook that outlines roles and actions to contain a breach

Blueprint for cybersecurity innovation

In this section:

Growing challenge: Data-driven innovation has increased cybersecurity risk because cybercriminals also continue to innovate.

Layers of protection: Integrating technological advances at each layer of a security strategy will help to strengthen your ability to react to rapidly evolving threats.

Bottom line: With threats to data constantly evolving, leaders must keep pace through innovative cybersecurity strategies.

Digital transformation is delivering opportunities for organizations to improve their business in a variety of ways. Increased mobility, big data analytics, and cloud services, among other emerging technologies and trends, are helping businesses run more efficiently, make better decisions, and improve customer experience.

But these advances create new vulnerabilities that bad actors are quick to exploit. Data-driven innovation has increased opportunities for cybercriminals to steal, expose, alter, and resell sensitive data — or even hold it hostage.

"We're in transition," says Brian Rexroad, vice president of Security Platforms at AT&T. "Ten years ago, we were focused on disk encryption on laptops. Now we're moving toward web-based applications as the primary site for data security."

An organization's sustained success, therefore, now hinges on its ability to be nimble in protecting and defending against all types of cybercriminals, from casual hackers to heavily funded nation states. With a security strategy that is grounded in innovation, you can develop the agility needed to face an always evolving threat landscape.

Unfortunately, not every organization has embraced a security strategy defined by constant evolution. In a recent survey of IT and business professionals, more than half said they have had the same model for information security management in place for three or more years — a lifetime in the rapidly shifting threat environment. Asked to grade their organization's security practices, just 11% gave themselves an A.[3]

"We're in transition. Ten years ago, we were focused on disk encryption on laptops. Now we're moving toward web-based applications as the primary site for data security."

Brian Rexroad
Vice President
Security Platforms
AT&T

If your organization's security strategy isn't making the grade, you're putting yourself at considerable risk. It's critical to deploy a cybersecurity model that can identify traditional and evolving threats and respond quickly to head off or help mitigate an attack.

50%

of organizations haven't updated their security strategy in 3+ years

Source: CIO/Computerworld

"As the bad actors continue to become more creative and advanced in their attack methods, we will be doing the same with our identification and defenses to mitigate whatever they're doing," says Alex Cherones, director of Threat Security Solutions at AT&T. "It's a game of cat and mouse."

Winning the game involves continually evolving your cybersecurity strategy and tools to stay in front of challenges that did not exist just a few years ago. It also requires allies that can help you to capture efficiencies and build end-to-end protection. The broader cybersecurity community is essential for sharing threat intelligence and improving the overall value of security to your business.

"You never want to be dependent on one layer of security, especially if you're protecting sensitive data," says Todd Waskelis, assistant vice president and general manager of Security Consulting Services at AT&T.

This report examines the primary layers of the data ecosystem in more detail, to help you prepare for emerging threats and agilely respond to attacks.

All data isn't created equal

Some of the data produced by connected devices or shared among workers involves publicly available or nonsensitive information. But there's plenty of highly sensitive data — customer and patient records, financial information, trade secrets, and other intellectual property — that is exposed to more risk simply because it is likely to be stored or transmitted outside of the traditional corporate firewall.

"Where and how data can be accessed has evolved," says Sundhar Annamalai, executive director for Integrated Solutions at AT&T. "Data can now be distributed on any device, anytime and anywhere. There is a new endpoint security posture paradigm that considers the identity of the user, their role within the enterprise, the context, and the current threat landscape."

That's why encryption is so powerful. By requiring a unique key or password to decrypt a file, encryption helps increase confidence about the integrity of a file's contents and the authenticity of its sender.

For example, encryption services can transparently encrypt individual email and document files as they travel from an employee's laptop to storage in the data center or the cloud. In a hardware-based approach, master encryption keys speed the encryption process and prevent online attackers from seeing the keys.

Some services can be deployed onsite or accessed as a cloud-based service. According to one recent survey, nearly three-quarters of IT leaders surveyed said their organizations have adopted at least one cloud-based security component[4].

Encryption is a potent element in any multilayered defense program. Without it, the confidentiality and integrity of your data as it travels back and forth, over a wide variety of networks, is in doubt.

Data

There's no shortage of data fueling modern business. The AT&T network carries over 135 petabytes of data daily. Global internet traffic surpassed 1 zettabyte — that's 1 trillion gigabytes — for the first time in 2016. Business traffic is expected to grow 18% annually through 2020[5]. Clearly, data is growing and evolving, creating ever-more opportunities for cybercriminals.

Enterprises once relied on static security perimeters to protect the valuable information that they stored in onsite data centers. No longer. With the blending of personal and business uses of devices and applications, data is scattered across mobile laptops, tablets, smartphones, and increasingly, IoT devices. Data is on the move with your employees when they visit nearby coffee shops or travel globally, creating new and unexpected avenues for attack.

Classifying your organization's various types of data, therefore, is one of the most fundamental decisions impacting the security of your data. Only after determining its level of importance in the organization can you know how the data should be secured.

See but don't grab. The growth of mobile workers notwithstanding, some data is simply so valuable or sensitive that it should never leave the heavily protected servers within a data center's walls. Organizations can implement technologies that allow users — be they internal

Innovation enabler: Identity & access management

Data protection strategies once focused primarily on verifying the identities of people seeking access. With growing numbers of smart devices, security systems must confirm their identities and also determine which assets they can access.

"Hackers and vandals are now so sophisticated it's nearly impossible for individuals to spot and stop threats," says John Donovan, chief strategy officer and group president for Technology and Operations at AT&T. "The network itself must become a security tool."

Identity and access management systems are designed to enable security teams to authorize people and devices to access data depending on a number of variables. For individual users, those variables can include the person's job title, department, location, the time of day they seek access, and the network they're using. Some of those same factors can apply to devices, along with controls based on the version of the mobile operating system installed and whether the device is configured with the proper security mechanisms.

Identity access and management solutions are also moving beyond the perimeter of corporate data centers. Large amounts of sensitive data never even make it behind a corporate firewall. For example, mobile and remote employees send data to and from cloud-based applications and storage.

To help protect this dispersed data environment, AT&T uses a software-defined perimeter approach to access control that restricts remote access to authorized users. Any IoT device, for instance, generally needs to communicate with a small subset of predefined users or devices. If a device attempts to move beyond those established parameters — a potential sign of malicious activity — its access is blocked.

employees working on PCs or mobile workers outside the firewall — to view the data but not actually transfer it to their devices' memory.

Control who, what, and where. Whether they allow data to just be viewed or permit it to be distributed, organizations must control who and what can see or download their data.

In the past, identity and access management tools focused on determining the roles and clearances of individual employees, alliances, or customers. Today, authentication and authorization must also be applied to devices and applications, not just people.

Encrypt to protect. Data encryption has long been a sore point for users because the encryption/decryption process was slow and frustrating. Advanced encryption algorithms, the general increase in processing power, and new encryption services are now making it easier to encrypt data by default, rather than by exception.

"It's essential that companies make things effortless for their employees," says Andy Daudelin, vice president for Cloud and Cloud Networking at AT&T. "If security is cumbersome, or performance is horrible, users will go around it."

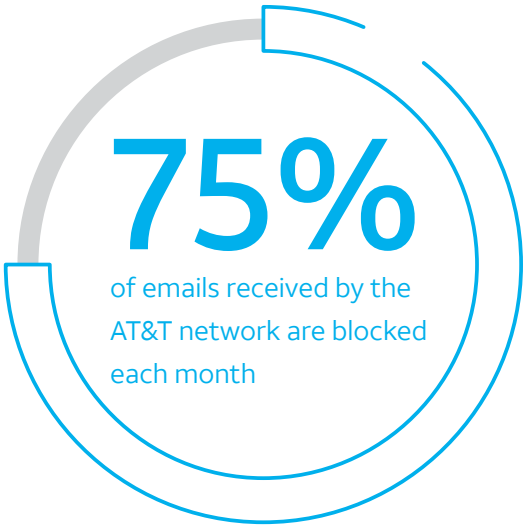
Look for services that can transparently encrypt individual email and document files as they travel from a device to storage in the data center or in the cloud. Some services are now embedding master encryption to speed the encryption process and prevent online attackers from seeing the keys. These services can be deployed onsite within customer premise equipment or accessed as a cloud-based service.

Applications

Well-known threats such as phishing and virus-laden email scams continue to flood organizations. Email remains an attractive target for hackers looking to breach corporate networks. In an average month, approximately three-quarters of the more than 21 billion emails transmitted to organizations across the AT&T network are flagged as suspicious and blocked from reaching their destination. That equates to more than 400 million spam messages detected by AT&T on its network every day.

Through social engineering schemes, cybercriminals use email attacks to steal employees' credentials, such as passwords and user names. Once they have tricked unsuspecting employees into providing the credentials needed to legitimately enter, the bad actors can take their time stealing your organization's most precious assets.

One well-crafted malicious email can have staggering results. In December 2016, a Ukrainian power grid fell victim to a cyberattack — the second in two years — that left more than 230,000 people living near Kiev without power for an hour. Russian hackers were able to access the network through phishing emails sent to government employees. Experts have stated that the cybercriminals seem to be testing their evolving capabilities[6].



Stolen data can be used immediately by attackers or resold on the dark web, months or even years after the original breach. These types of breaches disrupt more than the lives of individuals whose information was stolen. Cybercriminals use that data to access more sensitive information or tunnel into the businesses, government agencies, or military institutions where the individuals work.

Persistent mobile threats

Mobile apps are another emerging concern, underscored in late 2016 by the breach of more than 1 million Google accounts. By downloading infected apps from unauthorized app stores, Android users introduced the Gooligan malware that gained access to Gmail and Google Play™, among other services. At least 86 seemingly legitimate apps contained the malware. Security experts described the Gooligan attack as Google's worst account breach ever[7].

Unfortunately, employees find it hard to resist downloading apps from unapproved sources. Approximately one-third of all mobile devices are considered to be at medium-to-high risk of exposing sensitive corporate data[8].

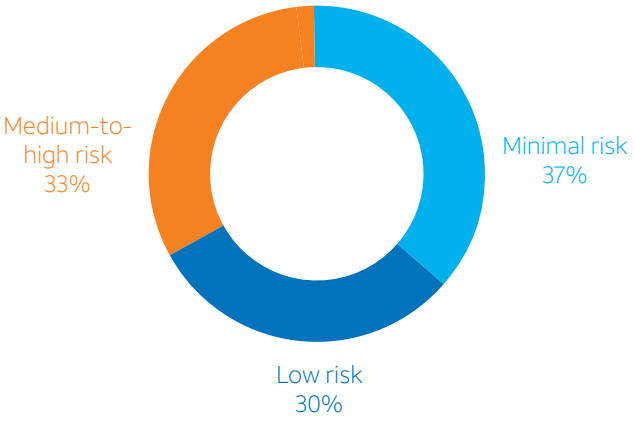
Other common applications can also expose an organization to risk. For example, the average company uses 49 cloud-based file-sharing services, accounting for 39% of all company data uploaded to the cloud. More than one in five documents uploaded to file-sharing services contain some sensitive data. But while 82% of cloud providers encrypt data when it's moving between a user and the cloud service, fewer than 10% encrypt data when it's at rest in the cloud — making it vulnerable to attackers[9]. The threat to data is further complicated by IT's unawareness of all file-sharing services used throughout the organization.

Secure-by-design. Whether applications are purchased off-the-shelf, developed in-house, or downloaded from the cloud, data security must

Mobile attacks advance

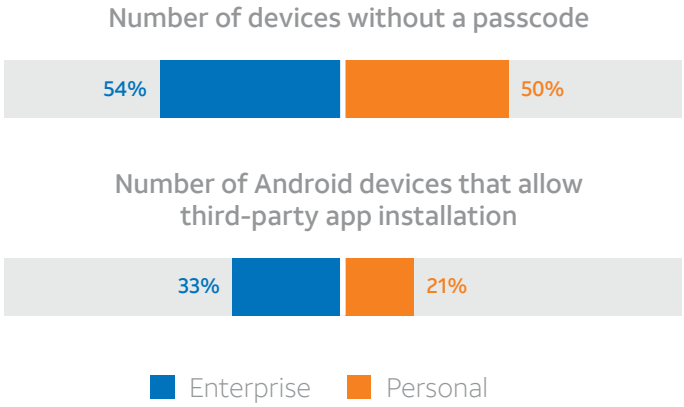
Many IT teams have difficulty pinpointing their mobility risk. Without this essential visibility, security personnel have no way to identify, quantify, or mitigate all risks to the enterprise.

One-third of devices have medium-to-high risk of data exposure



Risks from enterprise and employees' personal mobile phones

Employee behavior is the main reason mobile phones pose a risk to an organization's data. Devices that aren't secured with passcodes can be easily accessed by anyone at anytime. Malware can infect an organization's network through apps downloaded from unauthorized app stores.



Source: Skycure Mobile Threat Intelligence, Q3 2015

be built in at the start — not bolted on as an afterthought. This secure-by-design requirement has become increasingly vital given the massive quantities of data that modern-day applications generate and use.

Know the good guys. The advent of easily downloadable mobile apps has added complexity — and new vulnerabilities — to the application layer of security. Major app stores generally do a good job of weeding out malicious or poorly secured apps. However, even the reputable stores have sometimes been fooled by rogue developers who create malicious development environments designed to hide malware in apps that appear, at least superficially, to be safe.

Given this threat, organizations should create whitelists of approved mobile apps, and should closely monitor the app profiles of corporate-owned as well as bring-your-own devices (BYODs). That's no easy task. A recent analysis of global cloud usage data found that the average organization uses an astonishing 1,427 cloud services — each represented by an app on at least one employee's phone. Enterprise cloud services account for 71% of services used by the average organization, and consumer services account for the remaining 29%[10].

Counter the risks. Educating employees about the dangers of using unapproved apps is a necessary starting point, but organizations can't stop there. They need to deploy security controls — ranging from endpoint security

software to sophisticated threat analytics — and response systems to counter the risks posed by malicious apps and their related websites.

Control access. Among the most helpful solutions are a new generation of cloud access security brokers (CASBs). CASBs sit between your employees' devices and cloud service providers, serving to give organizations both visibility into the apps and cloud services employees are using, as well as a means to impose security controls on that activity.

1,427

The average cloud services used by an organization

Source: Skyhigh

CASBs, for example, could be configured to allow corporate-owned mobile devices to access certain cloud services, but to prevent less-secure personally owned devices from the same level of access.

Know the term:

CASBs

Cloud Access Security Brokers (CASBs) monitor apps and cloud services used by employees for enhanced security.

Look forward. Such externally applied controls may gain some inside assistance in coming years. Looking forward, future generations of applications and apps will likely have some level of self-awareness built in to help them act only within the parameters of accepted and expected usage profiles. In other words, applications themselves may soon control what types of activities and data access they'll allow, rather than passively waiting for an attack to materialize and then attempting to block it.

Innovation enabler: Threat analytics

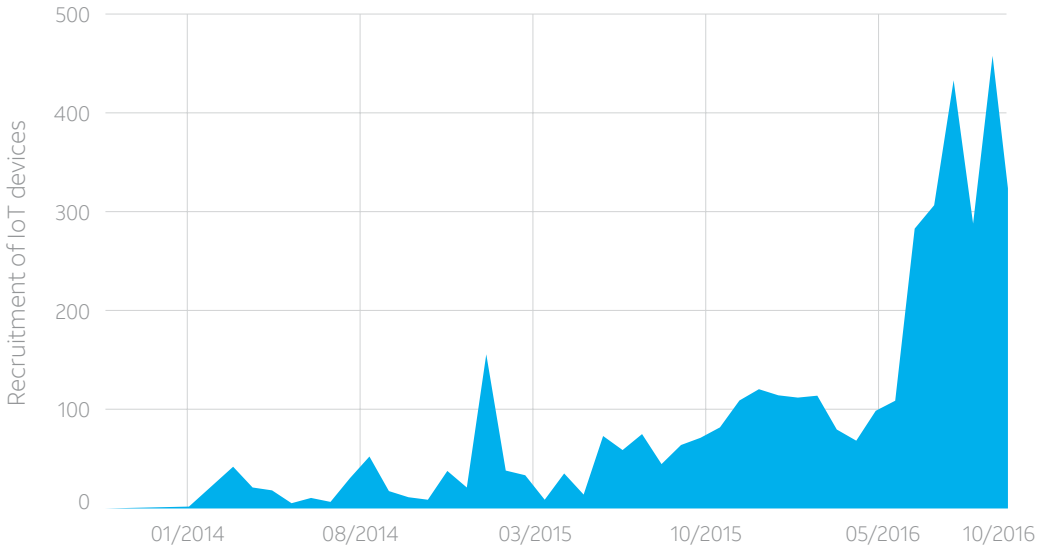
Detecting the potential threats hidden within an organization's mushrooming digital traffic is becoming increasingly difficult. Fortunately, automated threat analytics systems are highly efficient, faster, and more accurate than human security analysts are in threat detection and response.

For the most part, threat analytics systems function by recognizing known or potentially malicious data patterns and communications activities. The simplest threats to identify are previously observed attacks that exhibit known signatures. For example, if a system observes dozens or hundreds of password attempts before a user is granted access, it's safe to assume that the user is a malicious password-guessing program that should be blocked.

These systems can also flag behaviors or traffic that fall outside an organization's normal operations, bringing suspected threats to the attention of security analysts for more investigation. Some cutting-edge threat analytics systems are utilizing machine-learning capabilities to make educated guesses about whether an unfamiliar pattern or activity is likely to be a threat.

Threat analytics systems are proving their ability to sort through actual threats and minimize false positives. As a result, organizations are relying on them more and more to initiate automated responses to attacks before they can reach valuable data. Given that even medium-sized organizations can experience millions of security events each day, systems that can move beyond analysis and into automated response are serving a critical need.

Botnet activity rises as the IoT becomes a target



Since 2014, AT&T has seen a significant increase in botnet activity across its global network. In a DDoS attack, enslaved IoT devices — e.g., web cameras and DVRs — create a botnet that targets websites, routers, etc., to deny them service. In the six months leading to a large-scale attack on a prominent internet provider, AT&T detected a massive recruitment of devices that built the attack's Mirai botnet. While we can't predict what will happen, such recruitments provide insight into trends and lessons on future attacks.

Source: AT&T

Connected devices

A wave of IoT devices is sweeping across many organizations. The number of IoT devices is expected to rise from more than 6 billion in 2016 to more than 20 billion by 2020[11], including more than 12 billion IoT connections[12]. Wearable devices add another layer of complexity that security teams will need to protect as employees wear smartwatches, fitness bands, and the like to their workplaces. Nearly 215 million wearable devices are expected to be shipped by 2019[13]. Other types of connected devices — ranging from factory controllers to smart refrigerators — introduce significant challenges to protecting the data they generate, access, store, and transmit.

These devices are becoming increasingly attractive targets. Over the first half of 2016, we tracked a 400% increase in scans of IoT ports and protocols across the AT&T network — a clear sign that IoT devices were being recruited. A few months later, tens of thousands of IoT devices were commandeered to launch a series of major DDoS attacks on two large internet providers. The visibility that AT&T has into these types of developing attacks allows us to see trends and learn about new attack types.

DDoS attacks are just the beginning of a broader and more sinister threat enabled by the IoT. It's easy to imagine nation states marketing seemingly legitimate IoT devices that contain backdoors for breaching networks or monitoring their activity.

400%

increase in scans involving IoT devices in the first half of 2016

Source: AT&T

Raise the bar. Even though simple IoT devices may not produce or handle much sensitive data, it would be a mistake to assume they don't require protection. As the IoT-driven botnet attacks illustrate, unsecured IoT devices can be harnessed to launch DDoS attacks, which can then limit access to critical data that resides elsewhere. That's why even low-level devices should meet minimal requirements, for example requiring unique passwords and supporting software patches and upgrades.

Lock down BYODs. Traditional smartphone, tablet, and laptop devices raise a different set of challenges. Among the most persistent of those are the struggles organizations face

IoT standards schism: A security challenge

The Internet of Things has hundreds of protocols to address different aspects of the IoT ecosystem, including application development to machine-to-machine communications. In addition, a myriad of IoT standards is under development for different aspects of the ecosystem — from the device to the network to the application layer.

What's lacking is a common set of guidelines or practices applying these standards end-to-end for real-world IoT implementations, and especially, IoT devices. The current standards are highly distributed and fragmented, resulting not just in interoperability challenges, but in heightened security risks. By the end of the decade, more than 25% of enterprise attacks are expected to involve compromised IoT devices[14].

In the absence of widely adopted industry standards, many IoT device manufacturers fail to incorporate even basic security measures, and the devices arrive in the market with security flaws that make them attractive to hackers[15]. Even more vulnerabilities are added when one company designs an IoT device, another provides component software, another operates the network, and another actually deploys the device. It's often unclear who is ultimately responsible for security.

Enhancing the security of IoT operations depends in part on the emergence and widespread adoption of standards that recognize the entire IoT ecosystem. Some alliances are taking tentative steps to end widespread fragmentation in the IoT market[16]. One such effort includes an alliance of security providers and IoT experts joining to research and increase awareness on securing the IoT ecosystem.

With the development of best practices across the multiple layers of IoT, cybersecurity challenges and issues can be reduced for both organizations and individuals.

when they allow employees to use their personal devices to perform work tasks and access corporate data. As this BYOD trend continues to spread, so does the need for more corporate control over the use of these dual-purpose mobile devices.

Enterprises increasingly require that BYODs be configured with password protection and encryption, to mitigate the risks to company data stored on personal devices. If employees don't agree to these requirements, employers can simply block personal devices that lack the proper security profiles from accessing corporate networks and systems.

To increase security levels, two-factor authentication can be required to access an organization's data, such as demanding both a typed password combined with a fingerprint scan or some other biometric identifier.

Executives may want to institute greater control over access to sensitive data. Through granular control, they can limit access based on a device's operating system, its geographic location, and the security of the network over which it's communicating.

Network

When returning from a business trip to the United Kingdom, an executive's mobile device automatically connected to the Heathrow Airport Wi-Fi, which she had connected to on an earlier visit to London. Just one problem: The exec was in New York when the device connected to the "Heathrow" Wi-Fi. The network was a rogue network created specifically to trick devices into connecting without the users even being aware of the threat[17].

Rogue Wi-Fi networks at coffee shops, restaurants, airports, and other public locales are a growing concern. A recent analysis found that 7.5% of Wi-Fi networks were either malicious or used to mount a network attack at some point during the year[18]. Over a three-month period in 2016, nearly one-third of executive devices were exposed to a network attack[19]. For executives and employees on the move, device exposure can happen by joining a public network, a fake Wi-Fi, or an improperly configured network. That's why access to secure mobility should be a best practice followed by all organizations.

Consider the case of a government contractor that mysteriously began losing contract bids it previously had won consistently. An investigation later found that an employee had been sending project proposals via a local coffee shop's unsecured Wi-Fi network. An outsider was surreptitiously capturing the files during transmission and selling them to a rival firm, which used the proprietary information to undercut the contractor's bid and win the projects[20].

Know the term:

Rogue Wi-Fi hotspot

An unsecure Wi-Fi network that is often created by bad actors to steal or compromise sensitive data. These networks are easily avoided by using VPNs and end-to-end security.

Extend the private network. One way to avoid the risk of unsecured public Wi-Fi networks is to require mobile workers to access corporate systems via a virtual private network (VPN). VPNs establish highly secure links over public networks, enabling mobile workers to safely access and transmit corporate data from almost anywhere.

Divide to defend. Ideally, you should segment your networks to place highly sensitive data in areas protected with the highest level of security and access controls. More broadly, of course, you must protect devices, corporate data centers, and cloud services. The level of security present in each of these variants can differ significantly.

Educate on malicious Wi-Fi. As noted earlier, unsecure Wi-Fi networks raise particular concern. Organizations generally understand how to best protect their perimeter from data theft, but they must stay current on emerging threats such as unsecure Wi-Fi networks.

Employee awareness campaigns are central to reducing breaches from rogue Wi-Fi sites and eavesdropping bad actors. Employees should understand the dangers of connecting to unknown Wi-Fi networks and the importance of logging onto trusted websites only. In addition, they should steer clear of sharing valuable files or data online or in an email.

Keep current. Regular maintenance of device upgrades should be central to your IT team's security practice. All devices — BYODs and enterprise-owned — that connect to an organization's network should have the latest operating systems, security protections, and patches.

Safeguard machine-to-machine communications. The rise of IoT devices brings to the fore another form of networking: communications that can range from a robotic controller exchanging data with a factory

Innovation enabler: Virtualized security

One of the most impactful IT trends during the past decade has been the shift of hardware-based IT infrastructure — servers, storage, and networking equipment — to more flexible software-defined architectures that can be easily deployed, scaled, and managed. Among other disciplines, this trend has included software-defined networks and the virtualization of specific functions within those networks.

"Virtualization allows us to deploy security wherever it is needed," says Jason Porter, vice president of Security Solutions at AT&T.

Software-based or virtualized security is emerging as one of the most promising forms of network virtualization. By providing innovative solutions that can be deployed onsite as well as in private and public clouds, virtualized security helps protect an organization's data regardless of its location.

Instead of having to purchase, maintain, and integrate hardware-based security controls, virtualized security solutions can be deployed on a shared hardware platform. Virtualized security can rapidly adapt to changing security demands and easily distribute new security functionality.

One scenario in which virtualized security should prove useful is the increasingly common practice of applications running in both public and private clouds. Virtualized security can give organizations the means to implement consistent security controls and policies across all of those environments.

With data residing inside and outside of an organization's walls, virtualized security should be in your ever-evolving security tool chest.

automation system to the interaction between two cars traveling along a highway.

Organizations should put in place systems that help protect the data being exchanged, verify the identity of the communicating devices, provide needed management oversight across the entire IoT environment, and in some cases, inspect traffic for legitimacy.

Data center and cloud

To protect data inside their data centers, enterprises have built strong defenses with firewalls, spam filters, and other perimeter protections. Many have gone on to implement multifactor authentication and build threat analytics and response solutions. Organizations also are contracting with outside consultants and service providers to develop or deliver cybersecurity capabilities that they don't have the skills or resources to provide themselves.

Don't compromise on cloud security. As they tighten the security of their data centers, however, corporate data and applications continue their steady migration to services and data centers residing in the public cloud.

Innovation enabler: Incident response

Given the when, not if mindset that now saturates the cybersecurity market, you need to be proactive in how your team will mitigate cyberbreaches. That's where a sophisticated incident response plan comes into play.

Successful incident response plans begin well before a breach occurs. Along with the tools and teams required to identify and respond to breaches, an incident response program requires two core components:

A cross-functional team. A post-breach response is often an all-hands-on-deck affair involving the C-suite, IT, security, communications, legal, and other teams across the organization. Service and technology partners also play a role, as do law enforcement agencies, regulators, and, of course, customers.

Frequent testing. Just as your organization holds regular crisis management exercises for various scenarios, an incident response plan must be regularly tested so that all involved parties are crystal clear about their respective roles and responsibilities.

If the breach requires public disclosure, you also will need to soothe the concerns of customers, address media queries, and meet with regulators and law enforcement.

An incident response plan can make or break your business. Without an organized method of managing the aftermath of a breach, a company could lose tens or even hundreds of millions of dollars. But with targeted planning and regular testing, you can help to avoid that doomsday scenario.

Companies are currently uploading an average of 18.5 terabytes of data to cloud applications each month, but fewer than 9% of cloud providers have implemented enterprise-grade data security and privacy controls. That's a problem given that nearly 20% of files stored in the cloud contain sensitive data[21].

Organizations should require that their cloud service providers deliver at least the same level of data protection provided by their own data centers. Particularly for smaller organizations with less sophisticated security processes, third-party cloud services can offer rigorous in-house security protections.

But securing your data in the cloud is just the first step. One of the most daunting data protection puzzles is integrating corporate and cloud-based security models, while also working to ensure that data remains highly secure as it travels between the two.

Don't go it alone. There's a growing reliance on external cybersecurity expertise to help address the complex challenges introduced by moving applications and data to the cloud. By working with a cybersecurity service provider, your organization can improve reaction times to attacks and get access to innovative threat technologies and cybersecurity expertise.

Organizations also can tap into the shared knowledge and data on existing and emerging threats — acting as an early warning system to developing threats. Lessons learned by your service provider from an attack on one organization are used to respond and protect if a similar attack is launched on your data.

Clearly, the challenges of protecting data are as multifaceted and complicated as the digital landscape itself. Cyberattackers love this complexity because it means some security holes will be overlooked. To help close such vulnerabilities, organizations must take a comprehensive and systematic approach to protecting data in every data center, device, and application in which it resides, and on every network that it traverses.

Conclusion: Your call to action

Protecting your valuable data becomes even more important as business innovation increases your competitive advantage. Ever-eager cybercriminals are ready to exploit any new opportunities, including those resulting from your gains. To help defend your successes, AT&T recommends a strategic mix of innovative technologies and proven basic processes.

Identity & access management: With identity and access management systems, people and devices accessing your networks can be verified and authorization levels set for each.

- Security teams can manage the people and devices that can access data based on a number of variables.
- A new generation of software-defined perimeters holds promise to strengthen identity access and management by restricting remote access to authorized users of IoT or other devices.

Threat analytics: Advanced threat analytics systems flag behavioral changes in devices, services, and users accessing systems or applications on the network.

- Abnormal changes in data traffic patterns act as early indicators that a botnet, for example, has hijacked devices to launch a DDoS attack. Armed with this information, threat analytics programs can alert security teams or automatically respond to the threat.
- By relying on automated responses to evaluate and react to threats, your security analysts are freed to concentrate on other security demands.

Virtualized security: An offshoot of network virtualization, software-defined security allows you to follow and protect your data — onsite as well as in private and public clouds.

- Not only does virtualization save physical space, it also helps keep your cyberdefense technology current through regular software updates.
- Virtualized security provides the added flexibility to scale, depending on how much security functionality it needs.

Incident response: An incident response plan includes a detailed and comprehensive playbook that spells out the participants, processes, and lines of reporting that come into play should a serious cyberbreach occur. (For more on this topic, read The CEO's Guide to Incident Response.)

- Regular testing of an incident response plan helps ensure that your team knows their responsibilities and confirms that the plan is up to date.
- Standardized procedures enable quick reaction times when a breach is detected and mitigate damages from the attack.

The ongoing digitization of your organization creates many opportunities for innovation — and new openings for cyberattack. To sustain the competitive advantage resulting from your innovations, you must be able to protect your valuable data. Cybersecurity's evolution will help you in working to protect the data that is critical to the success and growth of your business.

Additional reading

- Cybersecurity Insights, vol. 1: What Every CEO Needs to Know About Cybersecurity
  www.business.att.com/cybersecurity/archives/v1

- Cybersecurity Insights, vol. 2: The CEO's Guide to Securing the Internet of Things
  www.business.att.com/cybersecurity/archives/v2

- Cybersecurity Insights, vol. 3: The CEO's Guide to Cyberbreach Response
  www.business.att.com/cybersecurity/archives/v3

- Cybersecurity Insights, vol. 4: The CEO's Guide to Navigating the Threat Landscape
  www.business.att.com/cybersecurity/archives/v4

- Executive Abstracts
  www.business.att.com/cybersecurity/abstracts

- Know the Terms glossary
  www.business.att.com/cybersecurity/terms

- Network Security Solutions
  www.business.att.com/enterprise/Portfolio/network-security

- More resources available at
  securityresourcecenter.att.com

Endnotes and sources

1. Morgan, S., Hackerpocalypse : A Cybercrime Revelation, (2016). https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report/
2. Skycure. Mobile Threat Intelligence Report, Q1 2016. https://www.skycure.com/wp-content/uploads/2016/06/Skycure-Q1-2016-MobileThreatIntelligenceReport.pdf
3. CIO/Computerworld. C-Suite 360 Special Report, IT Security's Looming Tipping Point. (2016, Fall). http://core0.staticworld.net/assets/2016/09/16/csuite360_security_fall2016.pdf
4. IDG Enterprise. 2016 IDG Enterprise Cloud Computing Survey. (2016, Nov. 1). http://www.idgenterprise.com/resource/research/2016-idg-enterprise-cloud-computing-survey/
5. The Zettabyte Era—Trends and Analysis. (2016, June 2). http://www.cisco.com
6. Zetter, K., The Ukrainian Power Grid was Hacked Again. (2017, Jan. 10). https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report
7. Kan, M., Android Malware Steals Access to More Than 1 Million Google Accounts. (2016, Nov. 30). http://www.csoonline.com/article/3146094/security/android-malware-steals-access-to-more-than-1-million-google-accounts.html
8. Skycure Mobile Threat Intelligence, Q1 2016.
9. Coles, C., Only 9.4% of Cloud Providers Are Encrypting Data at Rest. (2015, July 16). https://www.skyhighnetworks.com
10. Skyhigh Networks. Cloud Adoption & Risk Report. (2016, Q4). https://www.skyhighnetworks.com/cloud-computing-trends-2016/
11. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. (2015, Nov. 10). http://www.gartner.com/newsroom/id/3165317
12. The Zettabyte Era—Trends and Analysis. (2016, June 2).
13. IDC. IDC Forecasts Worldwide Shipments of Wearables to Surpass 200 Million in 2019, Driven by Strong Smartwatch Growth (Press release). (2015, Dec. 15). https://www.idc.com/getdoc.jsp?containerId=prUS40846515
14. Gartner's Top 10 Security Predictions 2016. (2016, June 15). http://www.gartner.com
15. Palmer, D., The First Big Internet of Things Security Breach is Just Around the Corner. (2016, July 1). http://www.zdnet.com/article/the-first-big-internet-of-things-security-breach-is-just-around-the-corner/
16. Linthicum, D., The 2016 State of IoT Standards. (2016, Sept. 14). https://www.cloudtp.com/doppler/state-iot-standards-2016/
17. Varun, K., Telephone interview with Dwight Davis, Nov. 4, 2016.
18. Skycure Mobile Threat Intelligence Group. Unpublished threat data (2016, Nov.)
19. Skycure. Mobile Threat Intelligence Report, Q2 2016.
20. Britton, J., Mobile Threats and Where We Are Today. (paper presented at the 18th Annual AT&T Cybersecurity Conference, October 24-25, 2016). https://www.att.com/att/securityconference/session-replay/vid5000615.html
21. Skyhigh Networks. New Skyhigh Networks Cloud Security Report Finds Growing Risk to Critical Business Data in the Cloud. (Press release). (2016, Nov. 17). https://www.skyhighnetworks.com

"Innovation is essential to success. At AT&T, we believe cybersecurity innovation is essential to sustained success."

Jason Porter
Vice President
Security Solutions
AT&T

MOBILIZING
YOUR
WORLD℠

att.com/security