The CEO's Guide to Data Security

Executive Abstract | AT&T Cybersecurity Insights | Volume 5

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.

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.

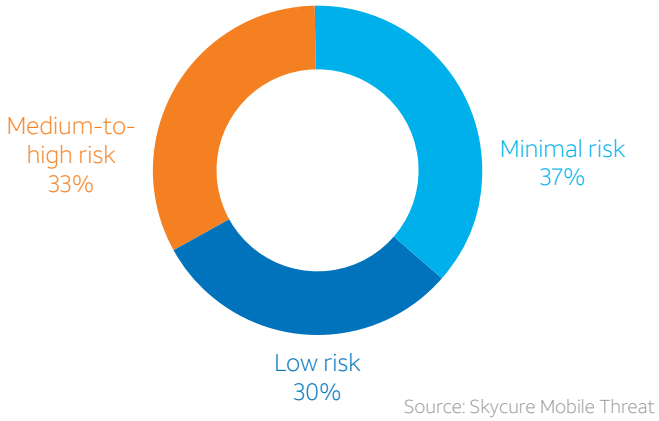
Cybersecurity innovation means keeping pace with cybercriminals by continually adapting and evolving your organization's security controls and practices for protecting enterprise data. Whether your data resides on an IoT device, a smartphone, a server behind the corporate firewall, or is in transit to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

Importantly, cybersecurity innovation also requires trusted alliances and integration into the broad and growing cybersecurity ecosystem. In today's environment, you can't fight organized cybergangs and nation-states on your own.

"Innovation is essential to success. At AT&T, we believe cybersecurity innovation is essential to sustained success," says Jason Porter, vice president of Security Solutions at AT&T.

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



Source: Skycure Mobile Threat Intelligence, Q3 2015

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

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.*

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

"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.

Data

Only after classifying the various types of data in your organization can you know how it should be secured.

See but don't grab. Some data is simply so valuable or sensitive that it should never leave the protected servers within a data center's walls. Organizations can implement technologies that allow users to view the data but not actually transfer it to their devices' memory.

*CIO/Computerworld. C-Suite 360 Special Report, IT Security's Looming Tipping Point. (2016, Fall).

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 the data.

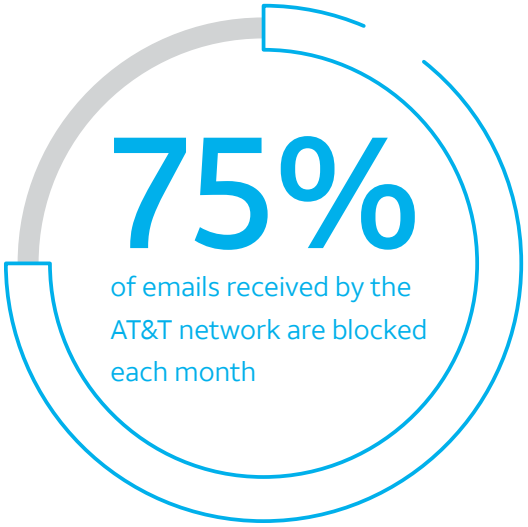
Applications

Common applications that can expose your data to risk include virus-laden emails, unsecure apps, and unencrypted data in the cloud.

Secure-by-design. For all applications — purchased off-the-shelf, developed in-house, or downloaded from the cloud — data security must be built in at the start and not bolted on as an afterthought.

Know the good guys. Organizations should create whitelists of approved mobile apps and closely monitor the app profiles of corporate-owned and bring-your-own devices (BYODs).

Counter the risks. Organizations 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.

Connected devices

Connected devices introduce new challenges to protecting the data they generate, access, store, and transmit.

Raise the bar. All IoT devices should meet minimal security requirements — for example, requiring unique passwords and supporting software patches and upgrades.

Lock down BYODs. Bring-your-own devices, such as employees' smartphones and tablets, should have password protection and encryption. Two-factor authentication can also be required to access an organization's data.

400%

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

Source: AT&T

Network

For employees on the move, device exposure can happen by joining a public network, a fake Wi-Fi, or an improperly configured network.

Extend the private network. Avoid the risk of unsecured public Wi-Fi networks by requiring mobile workers to access corporate systems via a virtual private network (VPN).

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.

Keep current. Regular maintenance of device upgrades should be central to your IT team's security practice.

Data center and cloud

Organizations are contracting with consultants and service providers to develop or deliver capabilities that they don't have the resources to provide themselves. A strong cybersecurity record should be a key factor in their selection.

Don't compromise on cloud security. Organizations should require that their cloud service providers deliver at least the same level of data protection provided by their own data centers.

Don't go it alone. By working with a cybersecurity service provider, you can improve reaction times to attacks and get access to innovative threat technologies and cybersecurity expertise.

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.

An evolving threat landscape

As technology evolves, the threat landscape continues to change. Consequently, organizations must continually evolve their cybersecurity strategies and tools to stay in front of challenges that did not exist just a few years ago.

Persistent mobile threats

A growing concern involves rogue Wi-Fi networks at coffee shops, restaurants, airports, and other public locales. These unsecure networks are freely available to the growing number of road warriors who conduct business from their mobile devices. 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.

Emerging risks to connected devices

Connected devices — ranging from wearables to factory controllers to smart refrigerators — are becoming increasingly attractive targets for Distributed Denial of Service (DDoS) attacks.

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.

Morphing challenges

Email remains one of the most common methods used 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. Another challenge: third-party cloud storage services.

MOBILIZING **YOUR** WORLD℠

Download the full report at att.com/cybersecurity-insights