The CEO's Guide to Navigating the Threat Landscape

Executive Abstract | AT&T Cybersecurity Insights | Volume 4

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. 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.

The majority of these threats are well known. AT&T threat intelligence data indicates 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.

The challenge lies with 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. It only takes one malicious email, opened by an unassuming employee, to deliver a dangerous payload that can lock up your systems or lurk, undetected, while the bad actors steal valuable data.

We aren't saying organizations can ignore the emerging unknowns of the threat landscape. But by tuning the bulk of your cybersecurity efforts to address known vulnerabilities, you can focus on the vast majority of cyberrisks.

"The majority of cybersecurity threats are known," says Jason Porter, vice president of Security Solutions at AT&T. "Defending against the known is a balanced, level-headed approach that better secures your organization."

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

The known threat landscape

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

Malware

The volume of unsolicited emails with detected malicious attachments increased 300% from the first quarter of 2015 to the same period in 2016. Depending on the day of the week, AT&T catches anywhere from a few thousand to more than 2.5 million malicious messages daily across its global network. Malicious activity trended upward from approximately 250,000 on July 1 to 1.75 million emailed threats on Aug. 30.

Ransomware

Ransomware has joined the list of known threats, as attacks have soared in the last year. In the AT&T Market Pulse: Global State of Cybersecurity 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.

Advanced Persistent Threats (APTs)

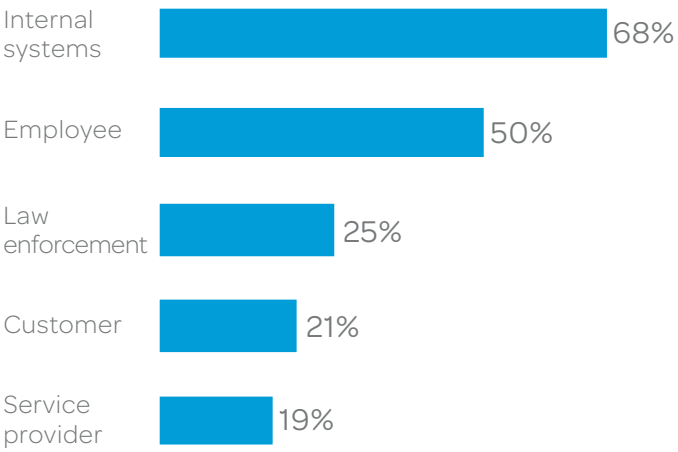
Attackers' ability to operate in stealth mode is becoming commonplace — and should serve as a wake-up call to security teams. The AT&T survey found that 65% of respondents in the financial services sector experienced more than one APT-related issue, followed by technology companies (69%). On a regional level, 69% of U.S., 66% of EMEA, and 70% of APAC organizations had an APT attack in the past 12 months.

Distributed Denial of Service (DDoS)

DDoS attacks have become common, with 73% of global survey respondents reporting at least one DDoS-related issue in the past year. Compared to respondents in the U.S., those from 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.

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

Emerging vulnerabilities

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 services, and mobile computing, while providing significant benefits to organizations, has also given rise to increased levels of cybercriminal activity.

Internet of Things

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. More IoT deployments create more possible points that hackers can exploit.

Cloud technology

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.

Mobile devices

Although the majority of security professionals express confidence in the security of their employees' mobile devices, about 40% admit that 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.

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

Preparing for the knowns

How to help protect your organization against the majority of cyberattacks

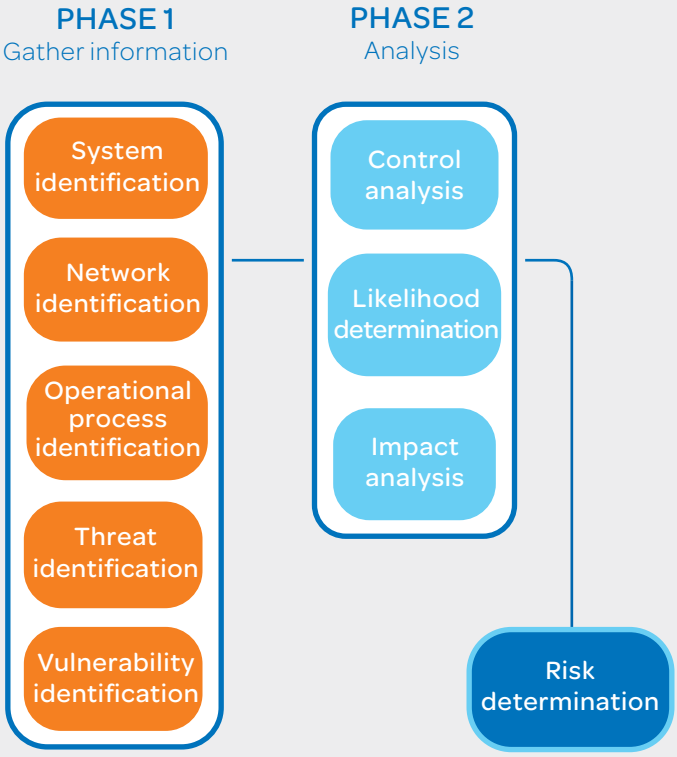
Harness technology

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.

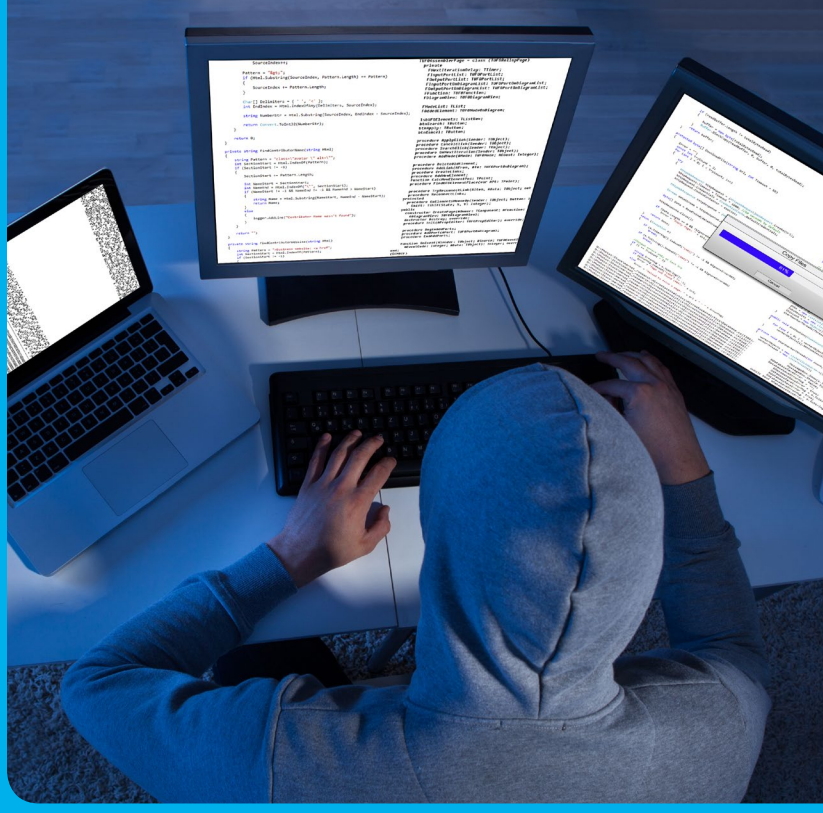


Priorities for emerging vulnerabilities

Developments in IoT, cloud, and mobile technologies have shaped business opportunities in recent years — and created new scope for criminal activity. Cybersecurity strategies, however, remain basically the same: tightening your current security initiatives, while recognizing the unique security demands of each new technology.

Securing IoT devices. Given how IoT data is likely to flow well beyond an organization's firewall, it becomes more vulnerable when handled by third-party vendors with less stringent controls. Risk assessments of your own IoT devices and policies as well as those of your third-party vendors should be included in your overall risk profile.

Defending your cloud. Key to your cloud strategy should be the security of your cloud service provider and the security of your connection between the cloud and your organization's network.



Locking down your mobile devices. A corporate edict that bans employees from connecting to unsecured Wi-Fi may be tempting but is unlikely to protect your organization's mobile environment. A robust mobile security strategy should be sensitive to user experience while folding mobile devices into your overall security strategy.

MOBILIZING **YOUR** WORLD℠

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