TANIUM

# Challenging times call for a cybersecurity plan of action

# Introduction

Could there be a more “exciting” time to be a cybersecurity executive? Some might choose other adjectives: stressful, uncertain, confusing, mind-boggling — to name a few. The past two years or so have seen an unprecedented string of events that have elevated threat levels and increased awareness of cyber risks at the highest levels of organizations.

Among the trends that have helped put cybersecurity in the spotlight are the dramatic rise in remote and hybrid work as a result of the pandemic; an ongoing and rapid shift to the cloud; a greater reliance on mobile devices in the workplace; a dramatic growth of e-commerce platforms and transactions; more sophisticated threats, including ransomware; a rise in the number of data privacy regulations; a worsening security skills gap; and an ever-growing threat surface.

The number and types of threats continue to increase, whether it’s malware, phishing, zero-day attacks, distributed denial-of-service, data breaches and others. Software vulnerabilities have become a major concern, so starkly illustrated by the recent flaw discovered in Log4j, the Java-based logging utility. Experts called the vulnerability, which involved arbitrary code execution in the framework, one of the biggest and most critical of recent years.

This eBook examines recent notable cybersecurity incidents, some of which made headlines and caused significant damage to the victim organizations, and all of which struck fear in many an organization — or should have. It also presents a strategy that organizations should consider adopting to build a strong cybersecurity program designed to defend against the latest threats.

# Security in the headlines

The past few years have seen some historic cybersecurity incidents, including large-scale ransomware attacks and advanced persistent threats (APTs) or data breaches across virtually all sectors. Here's a brief look at some of the key attacks of recent months:

In May 2021, U.S. oil pipeline system Colonial Pipeline, which originates in Texas and carries gasoline and jet fuel mostly to the southeastern U.S., **suffered a ransomware attack** that impacted systems used to manage the pipeline. Colonial Pipeline shut down all of the pipeline's operations to contain the attack and due to concerns about the attackers carrying out additional attacks on the pipeline. Within hours of the attack, Colonial paid the ransom demanded by the attackers. The incident was said to be the largest cyberattack on an oil infrastructure in U.S. history.

In June 2021, a **print spooler vulnerability** was patched as part of Microsoft's regular Patch Tuesday workflow. A few weeks later, around the July 4th weekend, a proof-of-concept exploit was released. Interestingly, this was an inadvertent zero-day release, as the bug it exploited was different from the original Common Vulnerabilities and Exposures (CVE). Not only that, but this vulnerability also impacted every version of Windows, server or workstation. Organizations scrambled over the holiday to quickly apply mitigations that were discovered to be insufficient. This highlighted the fact that organizations need scalable, fast solutions for identifying the presence of a vulnerability.

What happened to Kaseya, a company that provides software for managing networks and systems, in the summer of 2021 is the type of thing that keeps every vendor awake at night. In the case of Kaseya, **a supply chain attack** compromised the trust of its endpoint management tool to deploy ransomware. While about 50 different managed service providers were compromised, the overall impact hit more than 1,500 individual companies that had outsourced services to these providers. The attack, which was carried out by REvil, caused widespread systems downtime. It also led to the arrest of two individuals charged with deploying REvil ransomware to attack U.S. businesses and government entities.

Security researchers in December 2021 identified a zero-day security vulnerability involving **arbitrary code execution in Log4j,** a Java-based logging framework that is part of Apache Logging Services. Security experts said the vulnerability was among the biggest and most critical to be discovered in recent years. This bug affected a library used in thousands of applications — enterprise and free/open-source.

These are just some of the cybersecurity highlights — or, more appropriately, low points. Attackers have realized the massive opportunities for gain when going after large organizations or supply chains. As with any business, economy of scale is always the most profitable solution. This is true in cybercrime, too. While Big Game Hunting is on the rise, smaller businesses are often affected by spillover attacks or supply chain compromises.

When we think about the most concerning threats on the landscape, we often go to the newest vulnerability. But repeatedly, the attackers hide in plain sight, sitting in an organization's environment using an old contractor's credentials, the service account passwords that have not been rotated in years, or by social engineering legitimate users into facilitating access.

Older vulnerabilities are sometimes the most damaging. A 2021 study of vulnerabilities most exploited by ransomware actors indicated that vulnerabilities from 2013 to 2019 were used most often in high-profile ransomware attacks. And it's important to remember that insider threats are still a big reason attackers succeed. Phishing, vishing, stolen and reused credentials, and various forms of social engineering are so successful that they are used in many attacks.

Organizations need a plan of action to counter all of the threats. This plan should cover at least five key areas: inventory and asset management, breaking down silos, risk assessment, gap analysis and patch management. Let's take a look at each of these.

# Inventory and asset management

To find and stop security threats such as malware on endpoints, security teams need to be able to see these threats. But many organizations report that a lack of visibility is a challenge for their security operations.

Activities such as shadow IT, where employees procure devices, software or services without the knowledge or approval of central IT, only exacerbate the problem. And this will happen. People will use unknown devices and bring them onto the company network. While the intent is not malicious, the impact can be catastrophic.

Also, adding to the challenge of asset management are the remote and hybrid work models. Many employees use their own devices to access data they need to do their jobs.

Security teams can't identify, patch, or securely configure questionable endpoint devices when they don't even know they exist within the environment. All the threat hunting in the world does not make up for the assets they are completely missing.

To effectively manage IT assets, organizations can't rely on legacy tools that can take weeks to return results. They need results in real time and at scale across the entire network. Solutions such as converged endpoint and security management platforms provide security teams with real-time, actionable data across endpoints.

Endpoints are the most common point of entry into IT environments, which means effectively managing endpoint security is vital. It requires focus and vigilance.

## Breaking down silos

Another important practice is to break down any silos that might exist between the security and business teams. Unfortunately, the relationship between security teams and business users can be a bit antagonistic. Security professionals are looking to ensure the protection of systems and data, while users want to avoid any tools and processes — including those for security — that might hinder their work.

It's important for cybersecurity leaders to remember that while they are experts on security and technology, the business users are experts on how they use that technology to meet business goals. Working with, rather than against, them is critical, and security should be seen as a foundational service provided to all areas of the business. Security teams should exist to support and enable better experiences through secure design.

The exercise of mapping assets, software inventory and data at rest and in transit cannot be done from within IT operations alone. This is a unique opportunity to build alliances within the business, uncover gaps, improve work efficiency, and even save money.

It's important for security to build relationships with representatives across the organization, to gain their buy-in, and to establish a rapport and feedback opportunity as the security team implements and modernizes the architecture.

CISOs should consider creating a CISO Advisory Board to gather insights and feedback from business users.

They should form relationships with the people who can shine a light on shadow IT and keep security leadership aware as solutions are being evaluated. These valuable relationships enhance the adoption of new security initiatives, proactively alert security to problems, and enhance trust.

Working with business users also gives IT and security an opportunity to discover situations such as when three different business groups are each using separate cloud-based software tools to effectively accomplish the same goal. It unlocks a powerful opportunity to identify duplicate efforts, stale solutions or opportunities to consolidate tools and workflows across other teams — saving a significant amount of money.

## Risk assessment

Risk assessment is something organizations need, but it is not easy to do.

It's like accounting math, but for technology. The meanings can shift, and it is all predicated on a shared understanding of what the risk assessors are trying to do and how they are measuring risk.

Fortunately, there are some effective practices for risk assessment. One is to provide contextual understanding. Risk is, at its core, a relationship among vulnerability, threat and criticality. A risk assessment team might measure risk based on the presence of vulnerabilities, the likelihood the organization would be targeted by someone seeking to exploit those vulnerabilities, and how critical a targeted system is to the organization.

**Get a comprehensive view of risk posture and proactive ways to protect your organization from growing cyber threats with Tanium's Risk Assessment. Request your no-cost report →**

There are many risk measurement frameworks to choose from. The key is to map everything back to vulnerability, threat and understanding how important a given asset is.

Something else to keep in mind is that risk changes by the second. For every emerging threat actor, every zero-day vulnerability seen in the wild, and every laptop that logs on, risk has changed. The security industry has an antiquated view of risk as a snapshot in time, but that simply will not work in a technology landscape that changes so frequently.

Another issue is reporting risk. For many organizations, risk receives a single slide in the quarterly presentation to the board of directors — a situation where it's impossible to have meaningful conversation about the risk landscape and trends.

Organizations must create a measurement of real-time risk, and for that to be successful, risk calculation must be automated.

When instrumenting an environment, that should be a high-priority consideration.

The goal of understanding risk is to provide actionable insight for mitigation and remediation. Mitigation is the temporary state of reducing risk while planning for complete remediation or elimination.

Often, mitigation includes hotfixes, temporary access control changes, or other hardening steps that may reduce vulnerability but also impede productivity. This process is meant to buy time for proper remediation, which often includes upgrades or replacement of vulnerable assets.

In some cases, it's required that the business "accept the risk" by providing stakeholders contextual information about the cost of the remediation compared to the potential loss that exploitation of the risk would create.

While risk acceptance is a valid approach, it should be used with discretion and revisited regularly to ensure the organization has not assumed more risk than they are prepared to pay for.

At the end of the day, you must be confident that you have only written risk acceptance checks that you're confident you can cash. Bottom line: Risks must be mitigated, remediated, or accepted, and mitigation and acceptance should never be presumed as a "steady state."

# Gap management

For every security incident, there's likely a weakness of some sort within the attacked organization that cybercriminals were able to exploit. This is why it's so important to find existing security gaps and close them before it's too late. The time to update the environment is not during an attack; it's today.

Gap management in terms of network visibility and intrusion detection is impossible without knowing the current state and the end goal and measuring improvements over time. For starters, a company needs to establish how many endpoints it can see and manage compared with how many it can't, and set a goal to reduce that gap over a quarter.

As these goals are accomplished, the organization can expand on them, get more granular, and target specific, highly technical use cases.

While some of those more advanced use-cases may seem pressing, an organization that cannot confidently claim visibility of every endpoint must focus on visibility improvements as a first priority. Improving visibility scales the efficacy of every other effort for security and operations.

Detection, triage/analysis, incident response workflows, and infrastructure management are top-of-mind goals for organizations managing endpoint threats. To do these things effectively, enterprises must build in the right instrumentation before it's needed.

When assessing instrumentation, companies need to consider what they can get visibility into. Do existing solutions cover all the areas where visibility is needed? This includes endpoints, networks, applications, cloud services, and other areas.

# Patch management

For many organizations, patch management is still an Achilles heel, made worse by the rapid and unexpected shift to remote work. Even after all these months, some are still looking for the right way to get patches to the devices for which they have no line of sight.

Research shows that a relatively small percentage of organizations are capable of deploying a critical patch in less than 24 hours, and many are not confident that applied patches were successfully effective.

Vulnerabilities today are being actively exploited in the wild within hours, not days or weeks. Relying on a 30-, 60-, or 90-day patch compliance is clearly not enough for the more serious vulnerabilities.

In addition to understanding their overall patch performance, organizations need to identify and classify those IT assets that should be prioritized. But it's important to note that all systems are a priority to patch; it's just that some can realistically be allowed a little more time so that the most urgent can be patched first.

This is why understanding risk is predicated on understanding asset criticality. Operational decisions depend on a real-time contextual understanding of your environment.

For most organizations, this means identifying the public-facing systems, such as e-commerce sites, as a high priority since they are most vulnerable to attack. Then they can work inward and down to end-user workstations.

The tech industry often jokes that automation is born out of being annoyed with doing the same redundant, time-consuming tasks repeatedly. This is certainly true with patch management. While it sounds simple, practitioners know it's often fraught with missing devices, network limitations, and timing around business needs.

After visibility, your next most important priority should be ensuring your patches are automated. Doing so allows your talented engineering teams to focus on innovation and maturing to a proactive posture instead of spending dozens or hundreds of hours a month on retroactive patching.

## Conclusion: time to create and execute a plan

These are surely challenging times for organizations when it comes to cybersecurity. New threats and vulnerabilities are emerging all the time, while IT environments continue to get increasingly complex.

The fact is, it's not going to get any easier. Security executives need to lead their organizations in creating and deploying a plan of action that covers key areas such as inventory and asset management, breaking down business/security silos, risk assessment, gap management, and patch management.

By doing this, organizations will create an opportunity to strengthen their defenses against the latest threats. That will clear the way for them to compete effectively as digital businesses while at the same time protecting valuable information resources and elevating their security operations to a proactive and innovative level.

See how Tanium can help strengthen your organization's security defenses. **Request a demo** or test-drive Tanium in your own environment with a **free two-week trial.**