TANIUM | Public Sector

Protecting the IT attack surface while advancing digital transformation

Public Sector CIOs need the tools, processes, and trained personnel to protect their organizations from evolving threats

By Kyle Dewar, Director, Technical Account Management, Tanium

CONTENTS

Introduction

Today's public sector chief information officers (CIOs) face a daunting challenge: balancing the hard work of digital transformation with the requirement to protect their organization from sophisticated and potentially damaging cyberattacks. The current cybersecurity threat environment is exerting a lot of pressure on CIOs to manage risk by countering cyber threats with a combination of workforce skills and a portfolio of cybersecurity tools.

Responsible for overseeing all information technology in an organization, CIOs need to provide the IT guidance and resources an organization needs to support its mission and keeping essential services open.

Increasingly, that work involves digital transformation.

Almost always, digital transformation leads to a bigger, more distributed, and more varied IT infrastructure. To deliver more streamlined public services inevitably requires more cloud services, more use of data, artificial intelligence (AI) and machine learning (ML) operationalized by new applications that distribute the organization's digital footprint across a more distributed workforce through mobile devices and new application architectures, which likely involve application programming interfaces (APIs) and microservices instead of the monolithic applications developed a decade or two ago.

This eBook covers the challenges CIOs face in supporting innovation and IT security at the same time. It also explains some defense strategies that CIOs can adopt to protect the attack surface of their modern, cloud-first IT environments.

Understanding IT attack surfaces vs. attack vectors

In IT security terms, this more expansive IT infrastructure expands an orginization's attack surface. As defined by the Open Web Application Security Project or OWASP, an **attack surface** encompasses "all of the different points where an attacker could get into a system, and where they could get data out."

Protecting complex attack surfaces is difficult and often requires cyber tools that have complementary capabilities. Good cyber hygiene, effective configuration management that enforces cybersecurity policies, and continuous monitoring of cyber tool health form an organization's assessment of cyber-readiness.

Fifteen years ago, when most IT systems were on premises and protected by a network firewall, the attack surface was comparatively small. Today, when organizations rely on hundreds of cloud services and employees are working remotely, the attack surface is significantly larger. Every employee device on a home network is a potential attack vector that could lead to the compromise of mission-critical IT resources.

CIOs are responsible for keeping this distributed infrastructure secure. And they need to be thinking not only about external threats breaking through firewalls but also software vulnerabilities in applications that form non-linear threats like SolarWinds and WannaCry.

Log4j vulnerability and today's attack surface

That's the lesson learned from the **Log4j vulnerability**. Today's applications include hundreds or thousands of software components and services. A vulnerability in any of those components and services can jeopardize the security of the entire application and the organization that's running it. Having tools capable of adapting to emergent threats saves time, reduces risk, and increases an organization's cyber-readiness.

For example, many widely used versions of open-source logging utilities include a bug that allows attackers to submit a string to the logger's Java Naming and Directory Interface, allowing the unauthorized user to run code within the application with elevated privileges. This critical vulnerability exploit can be used to spread ransomware, exfiltrate data, shut down systems, and more.

The Log4j vulnerability, which received a 10 out of 10 rating for **criticality by NIST**, is frequently a key component found in web and application software, including about 4% of the most popular Java component repositories. The Log4j software artifact is found in applications, including leading commercial applications, as well as many home-grown applications developed internally. Thus, Log4j vulnerability is now a part of the organization's attack surface.

Log4j is a reminder of the major challenge CIOs face: selecting, deploying, and managing vast, complex IT architectures while identifying and mitigating all the threats in the attack surface of those architectures, no matter how complex or unfamiliar the threat may be while managing cyber readiness, reducing risk, and containing costs within a fixed budget.

Whatever the attack surface looks like today, it's destined to keep changing. In 2015, 30% of corporate data was in the cloud. By 2020, that percentage was 50%. The data suggests that migrations of applications, services, and data into the cloud will continue. These cloud migrations as well as other digital transformation efforts will contribute to an expanding attack surface with increasing complexity.

But if change outpaces security oversight, organizations will suffer. They'll fall victim to ransomware attacks, data exfiltration, business email compromise (BEC) attacks, and more. Operations might be disrupted. An organization might end up paying tens of millions of dollars in ransom, which subsequently jeopardizes public confidence - which no public sector organization wants.

This is the balancing act for CIOs: drive change while adapting to a continuously evolving attack surface to protect the organization's IT infrastructure. It's not easy.

Reducing the IT attack surface in the age of digital transformation

CIOs need a combination of tools, processes, and people for addressing these threats. Those tools and processes have some common requirements.

Real-time visibility

You cannot protect what you cannot see, thus CIOs can no longer rely on monthly or even weekly reporting to understand vulnerabilities and mitigate threats. Attack surface management requires access to real-time data and the ability to pivot from detect to respond at the speed of threats. Vulnerabilities can appear the moment a compromised endpoint connects to the network, or an obsolete software component is reinstalled from a backup. Cyber readiness should factor in current and approved software.

As much as possible, tools for monitoring endpoints and networks should provide real-time intelligence and support real-time investigations. Discovering that a system was compromised two weeks ago gives attackers too much of a head start. By then, ransomware could have spread across data centers and locations, or critical data may have been discovered and exfiltrated.

Easy to learn and easy to use

CIOs should choose tools that deliver critical cyber capabilities while requiring a minimal learning curve. If teams must secure new applications or services, give them tools that are not overly complex. Let them focus on the work they are doing instead of focusing on how to maintain complex or unwieldy tools. Talent and technology are key enablers to an organization's ability to accelerate response actions to emergent threats. This agility is critical as the cyber threat environment becomes more **volatile, uncertain, complex, or ambiguous**. Speed is a necessary component for the effective employment of cyber capabilities, which can be challenging for any public sector organization as the pool of cybersecurity talent is limited.

Another consideration: CIOs should choose tools that make it easier for security and operations teams to work together while responding to new threats. Security and operations teams need tools that let them pivot quickly to address whatever security threat is most urgent.

Comprehensive coverage

Choose tools that provide the broadest possible coverage of endpoints and other IT assets. Unfortunately, most vulnerability assessment and endpoint management systems overlook a significant percentage of endpoints—up to 20% in many cases. When IT can't see endpoints, they can't monitor and discover indications of compromise, nor can they include them on automated patch schedules. This contributes to poor cyber hygiene, endpoint configuration variance, and unhealthy tools that fail at the point and time of need. Endpoint visibility becomes the table stakes for an effective approach to managing a complex attack surface.

The attack surface includes all endpoints and systems connected to the organization's network. CIOs should make sure they can see the full attack surface, not just parts of it.

Centralization and automation

If possible, CIOs should choose tools that interoperate so that data can be visible, accessible, and understandable, and tasks can be automated across different computer security functional areas, such as threat detection and patch management.

Taking a "combined arms" approach and using multiple tools that work well together makes it easier to develop streamlined processes for security tasks. Automation becomes easier, too. The ability to pivot within a common platform can be instrumental to Security Operations Center (SOC) analysts because they won't lose time switching between one toolset and another to investigate incidents and mitigate threats.

Teams and talent

Tools are not the only part of a successful threat mitigation strategy. CIOs need a thinking workforce with the knowledge, skills, and abilities (KSA) to complete tasks within tight cycles that accelerate transitions from detect to respond to recover. This approach leverages tool capabilities to enhance organizational processes by synchronizing capabilities and processes to best protect the organization's evolving attack surface.

For example, organizations can use **Red Teams** and penetration testing against every part of their evolving IT infrastructure to discover new vulnerabilities before attackers do. The results from these exercises can then harden attack surfaces, while informing organizational learning processes. These "sets and reps" are invaluable learning opportunities that increase the KSA readiness of the cyber workforce.

Security and application development teams can include security subject matter experts in the design and planning phases of digital transformation projects, so that security is built into new products and services, rather than tacked on as an afterthought.

Zero Trust

CIOs should adopt a **Zero Trust strategy** to reduce access to the attack surface and to prevent attackers from easily traversing the network. In a Zero-Trust model, no user, process, or device is trusted without some form of interrogation. In other words, access to a network service or resource is not granted without examining device compliance, a user's roles, and successful authentication. In effect, everyone and everything is denied access, except for those users, devices, and processes that are authorized based on the organization's mission.

By closing unnecessary ports, IP addresses, and protocols, IT organizations reduce the size of their attack surfaces while increasing the difficulty for attackers to penetrate and move laterally across a network, searching for valuable data or spreading ransomware.

By leveraging Zero Trust security principles by default for digital transformation initiatives, CIOs can reduce attack surfaces and ensure that their new IT services and infrastructure are resilient and ready to enable digital operations. What features are important for a toolset intended for asset discovery and inventory?

CHAPTER 2

Applying kill chain thinking to reduce the cybersecurity attack surface

I'd like to draw on an important attack model called the kill chain. The U.S. military originally developed this model decades ago for analyzing capability gaps using operational data sets. A kill chain is a collection of sequential mission tasks or functions necessary to successfully employ a weapon against a specific target. Kill chains focus on outcomes by combining discrete capabilities to achieve synergistic effects. A kill chain used by the US Navy to evaluate air warfare capabilities consists of the following mission tasks or functions: find, fix, identify, track, engage, and assess. The desired outcome is to destroy a threat within a defined air space.

In 2009, in a technical paper by Lockheed Martin Corporation, several cybersecurity experts applied the kill chain model to the problem of defending against what was then a new form of attack: the advanced persistent threat (APT). A lot has changed since that paper was written, but the idea of kill chains is still useful. Here's why.

Before APTs came along, many people in IT thought that cyber defense could be boiled down to a simple checklist of tactics. If you wanted to block viruses, you deployed AV software. If you wanted to block intruders breaking into the network through unmonitored ports, you deployed a firewall and an intrusion detection system (IDS). And so on. Each of these solutions operated independently in silos to protect an area of the information network.

These simple security measures aren't wrong. They're just incomplete on their own. The rise of APTs made this obvious.

In an APT attack, intruders are willing to take their time. They'll poke and prod a network, find an opening, and deploy some malware. Next, they'll set up a command-and-control connection that gives attackers halfway around the world direct control of the malware that's been installed. Then they'll explore the network at their leisure. They might take days, weeks, or even months to find the valuable assets to steal or disrupt, depending on their purpose.

Stopping this kind of attack with a simple checklist of security steps is difficult at best and scales poorly as threats quickly consume limited IT resources. You need to see the bigger picture to understand how the attack's various moving parts are working together in subtle ways. Only then can you detect the attack and take action to stop it.

Kill chains and the modern cyberattack surface

This need for a broader vision of security is even more important considering the threats facing organizations today.

By comparison, in 2009, CIOs and CISOs were securing a relatively constrained and homogenous IT environment. Nearly all employees worked on site. Nearly all their desktops and laptops had been provisioned by the IT department, rather than being purchased by employees for their personal use.

Cloud adoption was in its infancy. Data centers hosted most applications under the watchful eye of local administrators. Network firewalls really could encompass most of the IT assets that needed protection. A CIO's kingdom really was like a castle: everything valuable in one central place surrounded by a secure wall with sentries watching for trouble.

Fast forward to today, and the attack surface is much larger, more varied, and more porous. The typical IT infrastructure spans multiple cloud providers as well as countless home offices with a mix of laptops, tablets, and smartphones.

Other endpoints include IoT devices and operational technology (OT) devices. Organizations had OT devices such as controllers on manufacturing floors before, but now they're connected to the internet to take advantage of the digitization of practically everything.

Another difference: The alarming **Log4j vulnerability** reminds CIOs that risks can come from the software building blocks used in purchased commercial applications. And those same software risks in the applications and digital services the organization supports itself.

In short, today's IT environment is complex, varied, and ever-changing. If simple, checkbox security measures were somewhat inadequate in 2009, they're wholly inadequate now.

That's why I think returning to kill chain analysis is so useful. It reminds CIOs that today's threats are sophisticated and complex and points out the importance of defending against every stage within the lifecycle of a cyberattack.

Understanding kill chain in cybersecurity

So what is a kill chain? It's a sequence or "chain" of events that together make an attack by a cybercriminal or nation-state more effective. As described in the Lockheed Martin paper, a cyberattack kill chain includes these seven steps:

1. Reconnaissance

The attacker surveils and explores the target, looking for vulnerabilities and gathering information such as hardware, software, identities, email addresses, or other information about the information network that might inform approaches or methodologies to probe, breach, or exploit a known or unknown vulnerability.

2. Weaponization

The attacker packages malware or RCE code in some way that can be delivered to initiate the attack. For example, the attacker might embed a remote access trojan in a Microsoft Office file or an Adobe PDF file.

3. Delivery

The attacker delivers the weaponized artifact to the target's network. They might deliver the file as an email attachment in a phishing campaign. Or an unsuspecting employee might download the file from a website or inadvertently copy it from a corrupted USB drive.

4. Exploitation

A user action or some other event triggers the execution of the malware. The malware takes advantage of vulnerabilities in the operating system or an application. One way or another, it slips through gaps in an endpoint's defenses.

5. Installation

The active malware installs itself on the user's endpoint or an application endpoint. Now the attackers have a presence on the internal network. In effect, the robbers are in the house.

6. Command and Control (C2)

In most APT attacks, malware on a compromised endpoint establishes a connection back to a remote system that serves as a controller for the attack. This command and control (C2) connection allows remote criminals, who may be thousands of miles away, to control the activity of malware on the victim's network.

7. Actions on Objectives

Now the attackers can proceed with whatever attack they have in mind. They might exfiltrate data from the user's system, or they might move laterally across the network, installing ransomware or exploring other systems for valuable assets to exploit. With the C2 connection in place, the attackers can basically do what they want, stealing or encrypting data, running PowerShell scripts, and so on.

This sequence might sound complicated, even laborious, but steps 3 – 7 can occur in just a few minutes. But a lot of APT attacks aren't fast at all. The attackers might decide to lay low and lurk on the network, exploring systems, installing more malware, or exfiltrating data at a trickle for months or even years.

CHAPTER 3

How to defend IT environments against the kill chain

This approach is intended to counter cyber kill chains used by adversaries. Recall that a kill chain is a sequence of interrelated activities necessary to achieve a desired outcome. Using the kill chain as a defensive planning tool involves looking at each cyber kill chain link to devise protection approaches that break the link.

Network defenders need to be perfect every minute of every day, while malicious actors only need to find one attack vector to successfully prosecute one or more chain links within a cyber kill chain to compromise a network. Applying cyber kill chains defensively is an approach to identifying capability gaps or blind spots in your cybersecurity ecosystem.

Kill chains are useful in decomposing complex problems into smaller, more manageable problems. By focusing on each link within the cyber kill chain, network defenders can achieve synergistic outcomes that improve the effectiveness of security tools and the overall readiness and protection levels of their networks. Conversely, breaking a link in the kill chain blocks an attack. This analysis will focus on approaches to block each link in Lockheed Martin's cyber-attack kill chain.

Defending against Reconnaissance

Reconnaissance is about gaining awareness of a target environment. In a physical sense, this involves identifying key terrain like hills that enable visibility or valleys that conceal movement. From the endpoint perspective, the network has key cyber terrain where adversaries can gain an advantage. Two categories of key cyber terrain would be services that advertise information about applications and application programming interfaces (API) that allow for remote access. Windows Management Instrumentation (WMI) is an example of key cyber terrain. Defending against reconnaissance from a cyber kill chain perspective would involve detecting new WMI subscriptions. Another example of key cyber terrain would be services like sendmail or SNMP mib information. Denying access to information from these applications has been a best practice for many years. Defending against reconnaissance involves identifying key cyber terrain, and then employing detection, denial, or defensive techniques to hinder or halt adversary reconnaissance activity. The desired outcome is a combination of information denial and detection of reconnaissance activities.

Defending against Weaponization

The weaponization step within the cyber kill chain relies on input from the reconnaissance step and is constrained by the third cyber kill chain step (delivery). Weaponization can be the sequencing of actions to exploit a vulnerability, the development of software artifacts to corrupt a software supply chain, or the introduction of malicious software into the blue network. While the act or process of weaponization often takes place on red or gray networks, the activity is tailored to the targeted blue network. Defending against weaponization centers on attack surface management, specifically reducing and hardening the organization's attack surface. In other words, this step in the cyber kill chain is about denying opportunity to adversaries. Removing the known vulnerabilities from the game board will increase the cost to the adversary while reducing blue network risk. Almost **60% of successful data breaches** take advantage of vulnerabilities in operating systems and applications that IT organizations knew about but didn't patch in time. One of the best ways of defending against the weaponization step in the cyber kill chain is effective and efficient patching operations that enable a high state of cyber readiness through cyber hygiene.

Defending against Delivery

The Log4j vulnerability illustrates how remote code execution (RCE) can be delivered using a web interface to access a vulnerability. Nefarious actors have other tools they can employ to deliver malicious code or actions. Firewalls and network segmentation can help channel attackers, helping focus where network defenders employ tools to block and detect delivery actions for data in transit. Defending against the delivery of malicious code is an imperative that requires active involvement from end-users, computer security practitioners, and physical security professionals. From infected USB drives to malformed browser requests to inadvertently visiting a compromised website, defending against the delivery of malicious code is a team sport involving user education, threat-informed physical security practices, and management of risk and resilience.

Defending against Exploitation

Defending against exploitation centers on identifying malicious software, preventing malicious software from executing, and/or remediating vulnerabilities to limit the effect malicious software can have on the system. These concepts are broken down to reputation services, application controls, and cyber hygiene. Cyber hygiene (patching, maintaining up-to-date software, and properly configuring software) is the best approach to prevent the **known knowns** within the attacker's toolbox. CIOs and CISOs can govern cyber hygiene practices in their organization by monitoring the right metrics like mean-time-to-patch or patching cycle duration. Visibility and control of endpoints at scale with speed are foundational to timely, accurate, and truthful data characterizing cyber-hygiene. Leveraging reputation services and antivirus software complements effective cyber-hygiene. The ability to identify deviations from normal behaviors, at-risk events, and indicators of compromise. While the former (cyber-hygiene) is about maturity and optimizing performance, the latter (hash hunting & detecting IOCs) involves agility and adaptability.

Defending against Installation

Security teams need real-time visibility into software installations and configuration changes on all endpoints, in all locations. Defending against the installation step within the cyber kill chain centers on preventing remote code executions (RCE). Stopping all RCE attacks can be a lot like stopping all crime. The array of actions available to prevent or hinder the detection of RCE attacks spans the continuum of antivirus and malware detection tools that identify malicious software signatures and alert on anomalies that indicate risk of compromise. Applying the installation phase of kill chain attacks should focus on the **unknown unknowns**, which encompasses unknown malware (potentially polymorphic malware), unknown file attacks, or cyber blind spots (things we do not realize that we do not know). One area CIOs and CISOs can consider is the development of an approved software list that leverages native OS tools like Microsoft's AppLocker. Additionally, reputation services can be used to aggressively identify malicious software. Combining technology with talent and techniques, CIOs and CISOs can leverage spiral development approaches to configure cybersecurity capabilities to detect, alert, or counter anomalies that indicate at-risk events or events that characterize compromise. Leveraging commercial or open-source intelligence sources to test, tailor, and tune alerts will generate an element of adaptability and agility within the organization's efforts to defend against the installation stage of the cyber kill chain.

Defending against C2 Communications

Security teams have a variety of ways to detect and block command and control communications. Firewalls and network monitoring tools can detect suspicious network activity, such as communications with an unfamiliar DNS server or an unusual remote host. Security teams can block many of these communications proactively by deploying Zero Trust controls that block all unauthorized communications by default.

Defending against Actions on Objectives

Defending against actions on the objectives centers on limiting access and denying the opportunity for a malicious actor to achieve their desired outcomes. In simple terms, the goal here is to lock every door and make the malicious actor work hard for each incremental gain. There is an assumption that the more work an actor does, the greater the potential they will be detected. Alerting on anomalous activity can be a challenge if alerts are not threat-informed and intelligence-driven. Consider applying **MITRE ATT&CK** or **CISA's Shields Up** as intelligence sources to guide security team meetings on developing relevant alerts. Endpoint security provides a final, critical defense against the kill chain.

To increase effectiveness, it's a good idea to make sure all the security tools providing these defenses work together seamlessly. Tools that complement one another can be instrumental in countering one or more links in the cyber kill chain. Data is a key enabler to generating a decision advantage; a data-ready platform that complements other tools while enabling visibility and control at scale with speed will deliver insight, confidence, and trust.

The Tanium platform for defending against kill chain attacks

At Tanium, we offer **a converged endpoint management platform** that delivers complete, accurate and real-time endpoint data regardless of scale and complexity. Our platform, available as a fast, flexible, and scalable cloud service, includes modules for:

- **Asset discovery and inventory**, helping IT teams find and track endpoints at all locations
- **Risk and compliance management**, including patch management
- **Threat hunting**, including tools for investigating and remediating threats before they disrupt operations
- **Client management**, including controls for managing and troubleshooting endpoints in real time
- **Sensitive data monitoring**, including auditing and automating access controls

Conclusion

Digital transformation is never done. To survive and thrive, organizations must continue innovating, launching new products and services and, optimizing old ones. As a result, every organization's attack surface will continue to change and, likely, grow.

CIOs need the tools, processes, and trained personnel to keep up with these changes and attackers' evolving threats, so that the organization's IT infrastructure always remains secure.

Know your IT risk posture:

Request a five-day, no-cost risk assessment to get a comprehensive view of risk posture across your organization.

Get risk assessment →

See Tanium in action:

Let us show you how Tanium's converged endpoint management platform gives complete visibility, control, and trust in IT decision-making.

Request a demo →

Tanium, the industry's only provider of Converge Endpoint Management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.