TANIUM

Public Sector

The ultimate guide to cyber hygiene for public sector agencies

Cyber hygiene is about proactively planning your security strategy to prevent cyberattacks, so you can keep services open.

The hybrid workforce has broadened the attack surface and cybercrime is becoming more sophisticated. Evidence of this is easy to find with a quick look at the latest news articles recounting the stories of government and private company networks falling prey to ransomware.

And the threats are only becoming bolder.

It's critical for organizations to deeply understand their risk posture and have tools in place that provide the endpoint visibility and control needed to detect and remediate threats. But tools alone are only half of the equation. IT leaders know that maintaining and securing enterprise networks requires pairing the right tools with hygiene best practices to yield the best outcome.

IT hygiene, or cyber hygiene, is fundamental to enterprise security and systems management. Improving cyber hygiene requires creating a process to continuously identify assets, risks, and vulnerabilities across an environment and fixing them with speed at scale. Focusing on cyber hygiene can help prevent many of the breaches, outages, and disruptions businesses fall victim to.

As environments become larger and more complex, device and workload variety increases. Organizations must manage everything from laptops and virtual machines (VMs) to containers across vast, distributed networks that span multiple offices and even continents. Under these demands, cyber hygiene often suffers.

In this eBook, we explain the components of cyber hygiene and how various tools either help or thwart efforts to improve it.

Know everything

To preserve and improve cyber hygiene, you need to know what assets you have. Do you have 50,000; 100,000; or 500,000 computers and servers in your organization? Where are they? What are they? What's running on them? What services do they provide?

Answering those questions is what asset discovery and inventory is all about. It's the foundation for cyber hygiene.

In this chapter, we dig into why that foundation is so important.

You can't manage what you don't know you have

To manage your endpoints, you need three levels of knowledge:

- What assets do you have, and where are they?
- What software is running on them, and is it licensed?
- How do the machines on your network relate to one another, and what is their purpose?

All organizations, regardless of size, need this information, which in modern IT changes constantly. Network assets come and go, especially with "bring your own device" (BYOD) a common and growing policy in many organizations.

Some assets may appear on the network only occasionally. With more organizations encouraging employees to work from home (WFH), complexity increases.

The operational disadvantages of not knowing

To paraphrase Don Henley, an American musician and former member of the band The Eagles, when you drive with your eyes closed, you're bound to hit something.

One of the first things you're likely to "hit" is a security vulnerability. If you can't manage an asset, you can't secure it. And you can't manage it if you don't know you have it. There may be attack vectors you're entirely unaware of — like an unpatched vulnerability.

How about financial implications? Do you have a general sense of what you're spending money on? Take software licensing for a popular program like Microsoft 365. If you have a license for 10,000 copies, do you use 20,000 or only 5,000? Do you efficiently use the license you pay for? Or are you out of compliance where you may be subject to expensive legal action?

Moreover, compliance isn't just about software licensing. Let's take healthcare as a use case. Healthcare companies must prove compliance with HIPAA and PCI provisions that cover protected health information and credit card data. Do you know where that data lives? If not, you can't prove compliance. The inability to prove compliance has two significant downsides: regulatory sanctions and unhappy customers.

What features are important for a toolset intended for asset discovery and inventory?

The tools or platform you use for asset discovery and inventory should possess:

- Accuracy
- Speed
- Scale
- Ease of use

Accuracy, speed, and scale are closely related. If it takes two weeks or a month to do an inventory, by the time you're finished, the network has changed, and you've undoubtedly missed something.

The bigger the network, the more of a problem this presents. That's why scale matters. Ease of use comes into play because a tool that's hard to configure produces errors, and people won't want to use it.

Older tools have a hard time with the demands of modern IT

Asset discovery tools built 10 years ago preceded many of the things modern IT environments operate with. They can't handle the rate of change we see now. Yet organizations often remain attached to tools they're comfortable with, many of which aren't easy to use.

In fact, they may take pride in mastering hard-to-use tools. Maybe they wrote custom scripts to make them work more effectively. Not only that, an entire vendor ecosystem has grown up around helping IT departments do just that.

The unintended and unfortunate consequences of that are IT policies and processes crafted not because they're the best way to address an issue but because they fit the capabilities of the tools in use. Entrenched tools become part of the IT infrastructure. But the best IT policies should be tool-agnostic. A tool built in 1993 or 2010 can't offer that flexibility.

Endpoint discovery is a constantly moving target

Not every endpoint on a network is a desktop computer, laptop, or server. There are printers, phones, tablets, and a growing number of consumer and industrial Internet of Things (IoT) devices. Mobile device management (MDM) is a growing application field. With an MDM provider like Microsoft Intune, you can track all the phones on your network.

But why should you have to worry about a consumer IoT device compromising the network? Here's why:

An employee of one of our customers was working from home. The company's security team was receiving alerts that someone was trying to break into her laptop. The source was a refrigerator with malware scanning her home network and trying to get into her device, which was temporarily on the corporate network. The same thing could occur with a smart light switch, thermostat or security camera.

No single asset discovery tool can identify every device type, so the tool or platform you use must integrate and work well with supporting applications that can recognize devices like phones, tablets, printers, etc.

Endpoint discovery is the foundation of Zero Trust solutions

When everything is a network device, everything is a potential security vulnerability. So you need policies and procedures that break endpoints into three categories: managed, unmanaged, and unmanageable. Endpoint discovery is the first crucial step in the trend toward Zero Trust, which is a security architecture that assumes no device or user can be trusted without verification.

Endpoint discovery is where cyber hygiene and security begin. You have to start there.

CHAPTER 2

Lock your doors and windows

Threat actors are getting better at finding weak links exploiting vulnerabilities and misconfigurations before security and IT ops teams know about them.

Regulatory pressure is also turning up the heat on organizations already struggling to manage the reputational and financial fallout of breaches.

At the heart of any good cyber risk management strategy lies vulnerability and configuration management.

1. Prioritize

The exponential growth in an organization's endpoints makes it impossible to immediately fix all issues. That makes effective prioritization important. First, it's about determining the criticality of your IT assets — laptops, servers, virtual machines, containers, or other endpoint types. This work can be slotted between the discover and assess phases of the lifecycle.

Use the results from your assessment to prioritize actions based on the criticality of assets and the vulnerability issues that affect them. Continuous visibility and monitoring should be watchwords here.

2. Focus on remediation

Timely remediation of vulnerabilities is essential because attackers act quickly and continue to get better at exploiting security gaps. While many security teams perform frequent scans and have good situational awareness of weak points, fixing them is another matter. Throwing people at the problem is not the answer. Even large IT teams can quickly become overwhelmed by the sheer number of issues and endpoints in need of remediation.

Automation keeps the lifecycle loop flowing smoothly. For teams worried about automated patches breaking critical systems, secondary evaluation processes can be built into automated workflows. These check whether patches are likely to be relatively benign or risky.

3. Track your remediation cadence over time

Understanding the speed and success of remediation reveals the effectiveness of your vulnerability management efforts. During the verify phase, you not only need to validate whether the required changes have been made but also evaluate the metrics of your performance.

You can see how quickly you identify issues, how fast your team addresses them, whether service-level agreements (SLAs) are met and how this compares to peer performance. Fresh, accurate data helps make this stage of the lifecycle more comprehensive and drives a culture of continuous improvement.

4. Automate everywhere you can

In an ideal world, you would automate the entire vulnerability management lifecycle. This would reduce manual error and cyber risk, accelerate time-to-remediation and free staff to work on other tasks. But there are still elements that some organizations may wish to, or be required to, perform, review, approve, audit, and validate directly.

These include the initial asset valuation piece, which can be more art than science, and analysis of metrics in the verify phase. Still, it's always worth periodically evaluating whether you could automate more.

5. Start small to overcome resistance to change

One of the biggest barriers to modernizing vulnerability management is people and culture. There may be staff members who are firmly against automatic remediations after having accidentally caused a production outage in the past through automated patching. There may be others who fear their jobs will be at risk if machines are used to fix endpoint problems. Some might simply complain "this isn't how things are done here."

Change can be frightening, but it's also essential to drive continuous improvement. Tackle the low-hanging fruit first. This shows reluctant stakeholders the value of automated approaches to vulnerability management and how much more productive it can make them.

Try something fairly innocuous to start, such as automating the discover to assess phases of the lifecycle. An automatic scan, triggered after discovering a new asset, could reduce a process that took five days to five minutes.

On the remediation front, consider implementing automated patching or software updates for medium- or lower-severity issues in non-production environments to demonstrate speed and effectiveness before moving to production environments.

6. Everything starts with policy

As important as technology is, let's not forget the basics, which begin with the right policies, plans and SLAs. It could be something as simple as: "We're going to develop a vulnerability management lifecycle that we define, and here are the SLAs for each cycle period." Once SLAs are in place, it may become clear that automated tools are the best way to achieve these goals.

7. Scan continuously for holistic risk reduction

Too often, organizations focus on meeting minimum compliance requirements without seeing the bigger picture — that effective vulnerability management is good for business.

It's important to ensure endpoint scans are not carried out simply to check the right regulatory boxes but as part of a holistic risk management strategy.

That means running scans continuously to identify, prioritize and address problems as they appear rather than just before an audit. Remember to cover the entire IT environment — not just fixed assets but also custom code in development.

CHAPTER 3

Respond faster

Responding to a cybersecurity incident, whether it's a data breach, a ransomware event, or one of several other types of cyberattacks, can dramatically compromise an organization's routine business operations, while shattering public confidence.

In this chapter, we offer the six-step PICERL framework, which organizations can adopt to improve and fine-tune their incident response plans. PICERL stands for Prepare, Identify, Contain, Eradicate, Recover and Lessons Learned.

Step 1. Prepare

Preparation ensures the right people from the right teams are involved, understand their roles, and know what they need to do when an incident occurs.

The preparation phase should generate a plan that incident response (IR) teams can practice. IR plans should be rehearsed so any weaknesses can be addressed. Mock drills help team members execute under the pressure of a real incident.

We ask customers if their IR team has participated in a drill and understood their roles. We also ask who notifies public relations, legal, and finance.

The preparation phase helps you determine whether you have the right tools. If not, do you have funding to procure them and provide training? Once an IR plan and budget have been created, it should be reviewed and approved by senior leadership.

Step 2. Identify

Once you have an incident, the identify phase is where you start trying to answer questions like:

- When did it start, and how did it occur: stolen password or asset, phishing email, malicious code from a portable drive?
- What was the point of entry? Was it an unpatched vulnerability?
- Who found it and how?
- What's the scope? Is it confined to one or two individuals or assets, or is it widespread?
- Can you continue to stay open and provide services? Will whatever steps you take impact different areas of the organizations' ability to stay open?

Very often, compromised credentials are the point of entry. And from there, the bad actors can take advantage of any opportunities they find.

Step 3. Contain

Containment is about executing your plan to prevent the unwanted behavior from spreading. A short-term containment strategy could be as simple as issuing a quarantine command to keep an asset, application, or system from communicating with anything except a security tool.

Long-term containment is a fix that's implemented organization-wide but may be short of completely remediating the incident's root cause. This could be a tactic for assisting law enforcement or regulatory agencies. It's a good idea to have long-term containment strategies connected to your data backup and recovery systems.

Patches and updates are also part of containment. Do you have unpatched vulnerabilities related to an incident? If so, it's time to accelerate the patch schedule for the application or operating system software in question.

This is also a good time to revisit which users have administrative access and to what systems. What is your attack surface relative to Active Directory? Have you enabled multi-factor authentication? These are all issues relevant to containment.

Step 4. Eradicate

Now you're trying to eliminate the cause of the breach — root and branch, as they say. That means in the case of malware, for instance, that you've found and securely removed every instance you've identified. You've hardened and patched systems where applicable. You've reimaged systems you can't harden. You've updated your threat intelligence to make sure you can identify artifacts related to the breach.

While the process unfolds, it may change the scope of your efforts. After a ransomware attack, for example, you may have a lot of systems that need to be reimaged and restored from their last known good backup. And if you don't catch all the artifacts related to the attack or you haven't addressed the vulnerability that was exploited to get in, you could be attacked again.

The key to eradication is thoroughness. Did you find it all (whatever "it" is being the ultimate question)? Often a partner or third party with specialized expertise can help with cleanup.

Step 5. Recover

The damage has been done; now it's time to focus on healing. You must be very honest with yourself. When can you return affected systems to production? Have you patched, hardened, and tested them? Have you used your red team (a group that plays the role of an enemy) to run a simulated attack against these systems using the same techniques as the attackers? You want to be able to say, "We addressed the vulnerabilities, and here's proof."

Recovery also means defining how the incident will change the scope of your monitoring. How long will you monitor for the activity that caused the breach: 30 days, three months, six months? And what will you look for? The red team tests will help, and so will the artifacts collected during containment.

Mean time to remediate

Mean time to remediate (MTTR) is how long it takes to move through the identification, containment and eradication phases of your IR plan.

In 2018, the Verizon data breach report found an MTTR in the range of 14 to 30 days for high-performing organizations. But there's a strong trend among security professionals to lower that number as IR plans mature and teams become better at practicing them.

Step 6. Lessons learned

This step should begin with an after-action meeting that includes everyone who was part of the incident response team: IT, compliance, legal, PR, etc.

This is where you have the opportunity to review and document what you learned about the breach.

- What part of your IR plan did or didn't work?
- Were there gaps where additional people were needed? Did you need to reach out to a third party or an internal team not on your list of resources?
- Based on the incident, do you need to change how you operate? Were you using the tools you had effectively? Were they configured properly?
- How was communication among teams? Could it be improved?
- Was there an employee aspect to the breach, such as a phishing attack or improper data handling? Can this be addressed with training?
- Was the vulnerability exploited endemic to a specific department or unit, or present across the organization? Could you address the vulnerability with a different operational structure or process?

The more flexible the IR plan, the more you'll learn from a breach when it occurs. Everything you learn should feed back into the preparation phase, which can always be refined and improved.

Conclusion

The reality is, ransomware and other cyberthreats are here to stay. Highly sought-after networks and critical infrastructure will always be a target. The intent of this eBook was to provide a broad, conceptual understanding of what cyber hygiene is as well as some hygiene guidelines, best practices, and insights to consider that will help prepare IT teams to defend the endpoints they manage more effectively.

The pivot from insight to action is where cyber hygiene often breaks down. Information is lost between the cracks of fragmented tools and teams.

Effectively coordinating patch and software deployments across an environment requires that IT ops and security teams be aligned, collaborative and accountable. This requires that key systems must be in place and shared workflows clearly defined.

A cyber hygiene assessment offers visibility into the health of your IT environment so you can understand the state of your endpoints, identify critical gaps, and learn how you can improve your cyber hygiene to decrease your organization's chances of becoming the next headline. Tanium can help.

Work with our experts to define an actionable path to better endpoint management and security with a **no-cost risk assessment.**

Learn more about how Tanium provides high-fidelity endpoint data and analytics to inform critical IT decisions at tanium.com →