TANIUM

No Industry Is Safe From Cybercrime

Defending Your Organization From Attack

Table of Contents

The Mandate: Prepare for an Attack

2020 showed us just how inhumane cybercriminals can be. The world experienced a pandemic of unprecedented scope. Organizations and individuals scrambled to adapt to the new reality. Service-based industries did everything they could to save lives and take care of the most vulnerable members of society.

When all of this was happening, cybercriminals took advantage of the chaos. They launched new attacks to exploit work-from-home vulnerabilities. They updated their standard threats with pandemic-themed messaging. And they targeted specific verticals at their most vulnerable moment.

This ebook will help show you how to stay secure, regardless of whatever comes next.

It provides insights and advice from security leaders who worked within two of 2020's most-targeted verticals — healthcare and education — to teach you how to best defend yourself when cybercriminals turn their attention towards you.

It will explore:

- Why and how criminals targeted specific verticals at different points in 2020.
- How to defend your organization when criminals target your vertical.
- How Tanium can protect you when you're most vulnerable.

Why and How Criminals Targeted Specific Verticals

When the pandemic first struck, criminals weren't picky. They employed a shotgun approach to exploit any organization they could.

> *"Because this was a pandemic, it really opened the attack surface across the world. Cyber adversaries weren't very selective. They were looking for easy money."*
>
> Jon Oltsik, Senior Principal Analyst and Fellow, Enterprise Strategy Group

"Because this was a pandemic, it really opened the attack surface across the world. Cyber adversaries weren't very selective," says Jon Oltsik, Senior Principal Analyst and Fellow at the Enterprise Strategy Group. "They were looking for easy money."

But as 2020 progressed, they did become more selective. They sought easy money in specific verticals. The first and clearest example: healthcare.

Attacks against healthcare providers increased dramatically once the pandemic began.

"It was really sad to see, but the attacks on healthcare institutions — providers and insurers — went up exponentially," Oltsik says.

Cybercriminals targeted providers when they were most overwhelmed by COVID.

"Organized crime groups were going after hospitals and healthcare providers in the worst affected countries that were in the middle of responding to the pandemic," notes Kris McConkey, Cyber Threat Operations Leader Partner at PwC. "The bad guys were doing that because they knew they were likely to get a quick payout."

Another less obvious example of a highly-targeted vertical in 2020 is education. Attacks against educational institutions actually decreased when the pandemic began. "The beginning of the year, up until about March, looked about the same as the prior years," says Douglas Levin, Founder of the K12 Security Information Exchange. "But with COVID arising in the spring, things quieted down a bit."

But cybercriminals weren't showing mercy to schools. They were just waiting for a better time to attack. And they found it during the back-to-school rush.

"With the school openings in August and September, we saw an extraordinary explosion of incidents," Levin recalls. "Since I've been tracking school cybersecurity incidents, I'd normally see an incident every two or three days affecting a school district. Since the start of the school year, I've seen at least two incidents per day occurring in school districts — including weekends."

The pattern is clear. Cybercriminals targeted education and healthcare when they were busiest and least able to devote meaningful attention and resources to cyber defense. But thatI isn't the only pattern we can draw from these highly targeted verticals.

Cybercriminals also targeted both verticals with ransomware attacks.

"The typical attack on healthcare was ransomware," comments Oltsik. "At the same time these healthcare facilities were overburdened with patient care, they were attacked and their systems were sometimes unavailable."

"The impact was severe," says Oltsik. "Their systems went down. Mostly administrative and not clinical systems, but those went down, too. So, patient care was compromised. A lot."

> *"The impact was severe. Patient care was compromised. A lot."*
>
> Jon Oltsik, Senior Principal Analyst and Fellow, Enterprise Strategy Group

And they used ransomware to cause similar havoc with educational institutions.

"A notable example is the Clarke County School District, which serves Las Vegas," says Levin. "The district experienced a ransomware incident in which the malicious actors also exfiltrated data about employees and students. If the school district didn't pay the ransom, the actors threatened to not restore the downed systems and to release data on students, educators, and students' families to the dark web."

These examples and many more reveal that, when criminals target specific verticals, they:

1. don't care who you're or what you do. If they can make an easy dollar off you, they'll see you as a rich target and nothing more.
2. will lock up your systems in the moments when you're most overwhelmed and maintaining operations is critical.
3. will launch a complex ransomware attack — that includes data exfiltration — hoping that you'll just pay quickly to resolve the incident.

This knowledge can help you define how to secure yourself when your vertical and your organization are most likely to be targeted and least capable of mounting an effective defense.

How to Prepare Before You're the Target

To produce this eBook, we spoke with multiple security leaders. Many of them worked with high-target verticals throughout 2020. They secured their organizations or their clients in moments when they came under heavy attack.

And they all agree on a few fundamental actions that organizations must take to defend themselves when cybercriminal target their vertical.

First, organizations must assume their vertical will eventually come under attack.

A few verticals generate most of the cybersecurity headlines: Finance. Technology. Government. And, yes, healthcare. But cybercriminals will attack anyone who can pay. And that includes verticals that don't get much press and don't look like good targets.

Consider the education vertical.

"The first big myth people have is that schools aren't interesting targets for cybercriminals," says Levin. "If they're interested in stealing money they'd go after a big corporation, hospital, or financial institution."

But even verticals that don't seem "interesting" commonly have the capacity to pay ransoms.

"While school districts always feel like they don't have enough resources, they still run very large budgets," explains Levin. "They're managing facilities, bus service, food service, and they employ a lot of teachers and support staff. Schools actually manage a lot of money and are attractive to cybercriminals."

In short: If a vertical manages a large budget, they'll always be interesting to cybercriminals.

Second, organizations must assume they'll be targeted when their vertical is targeted.

Only huge breaches make headlines, making it seem like only the biggest, best-funded organizations will be targeted. But this isn't true. Once again, consider the example of educational institutions.

"We know all about the big city school districts that serve hundreds of thousands of students," notes Levin. "But the majority of school districts in the U.S. are smaller and much more rural. Many people in those school districts tend to think they're just a small needle in the haystack and they'd never be targeted."

Unfortunately, that's not the case.

"Cyber adversaries are simply searching the internet for vulnerable systems," Levin says. "When school districts have older systems that might not be patched well, cybercriminals see that and can take advantage of it."

> *"When school districts have older systems that might not be patched well, cybercriminals can take advantage of it."*
>
> Douglas Levin, Founder, K12 Security Information Exchange

Cybercriminals are less ambitious than headlines make them out to be. When they target a vertical, they'll breach any organization in it that they can.

"They don't particularly care about the organizations they're targeting," cautions Levin. "They just need to know they can put an organization behind the eight ball so it will have to pay to have access to their devices and get their data back."

Third, organizations must develop a strong negotiating position against ransomware.

The threat of ransomware is only growing, in size, sophistication, and potential costs.

“Several years ago, the size of extortion demands being asked of school districts might have been $5,000 or $10,000,” says Levin. “Recently, amounts have gone up dramatically. They’re easily north of $100,000 or $200,000. And I’ve heard of school districts paying much more than that — even in excess of a million dollars.”

To avoid paying ransoms, organizations must construct a strong negotiating position, which means developing a number of capabilities.

“If you’re thinking about entering into negotiations with threat groups, it comes down to several factors,” outlines McConkey. “Do you have really good visibility into your IT environment? Can you tell precisely what the bad guys touched, what they accessed, and whether they still have a foothold? Based on the visibility and control you have, how confidently can you kick them out and keep them out?”

The need for these capabilities is also growing.

“All those factors really must go into planning in advance of an attack,” says McConkey. “Knowing how much visibility you have and how you’ll react when an intruder gets in and being able to use the dwell time to spot that they’re there and then kick them out and batten down the hatches. That’s becoming a significant focus for most organizations in their security planning.”

The lesson here: Organizations must develop ransomware defenses before their vertical comes under attack or they’ll have to pay an increasingly large and painful ransom.

Here’s how they can do just that.

Five steps to effective, efficient defenses

Assume your vertical and your organization will be targeted. And be prepared to fight back if that worst-case scenario happens. To help, we've developed a simple five-step process you can follow to defend yourself:

Step One: Assess your gaps and define your risk

Step Two: Button up your IT hygiene

Step Three: Develop a strong negotiating position

Step Four: Make your defenses as efficient as possible

Step Five: Re-evaluate your endpoint management and security tools.

Ask yourself: If we did suffer a ransomware attack, which critical systems would a cybercriminal most likely lock up? What sensitive data would they exfiltrate and threaten us with?

Step one: Assess your gaps and define your risk.

Ask yourself a few questions to determine when criminals will most likely target your vertical and how well you'll be able to fight back when they do.

- ✓ Does my vertical already have known periods of being targeted by attackers?
- ✓ Are there times of the year when organizations in my vertical are particularly busy, distracted, and less focused on security?
- ✓ Could my organization pay a hundred-thousand-dollar ransom — or a multi-million-dollar ransom — even if we don't consider ourselves a "rich target?"
- ✓ Does my organization have known vulnerabilities that cybercriminals could find through simple automated scans?
- ✓ If we did suffer a ransomware attack, which critical systems would a cybercriminal most likely lock up? What sensitive data would they exfiltrate and threaten us with?
- ✓ Could we rapidly evict an attacker, or would we have to pay their ransom?

Step two: Button up your IT hygiene.

You can't control when your vertical comes under attack. But you can control if your organization looks like an easy target. To reduce the chances that your organization will enter the crosshairs, you must eliminate the open vulnerabilities in your environment that cybercriminals will search for.

These open vulnerabilities are commonly simple things like unpatched endpoints.

> *"There's this perception that most hacks are done by nation-states on shiny zero-day vulnerabilities. But it's normally the most fundamental IT hygiene issues that lead to breaches."*
>
> Scott Lowe, Managing Director and Founder, EndpointX

"There is this perception that most hacks are done by nation-states on shiny zero-day vulnerabilities," says Scott Lowe, Managing Director and Founder at EndpointX. "But the reality is most happen because a server hasn't been managed or patched or there is a vulnerability on a browser. It's normally the most fundamental IT hygiene issues that lead to breaches."

Take care of the basics. Patch your systems. Update your applications. Configure your devices properly. And do so for the assets in your environment.

"I talk with CISOs and CIOs who say, 'I have 84% of my workforces' machines patched' or '92% of my devices are in-line with company policy,'" says Chris Hodson, global CISO at Tanium. "Well, unfortunately, it only takes one weak point in any organization to be compromised and used as a vector to move laterally and propagate across an organization."

Step three: Develop a strong negotiating position.

Ransomware is a complex, multistage attack pattern. To develop an effective defense, focus on the fundamentals of visibility and control.

"Any organization's ability to respond rapidly to an incident, investigate what happened, and actually take action to resolve it is going to be severely compromised if there isn't good endpoint visibility and control," warns McConkey.

To avoid that scenario, you need the ability to:

- See all endpoints, applications, and data in the environment.
- Confidently evict an attacker without paying their ransom.
- Know the attacker is gone for good and can't strike again.

Once you develop these capabilities, test them.

"Organizations really need to think about how to stress-test their response process and systems in this new world," emphasizes McConkey. "We have new and very extreme types of threat categories that exert all sorts of pressures organizations aren't accustomed to handling. Making sure you understand where the pitfalls are and how to bounce back from them very quickly is really important."

Step Four: Embrace distributed operating and security models.

For some organizations, this step will be optional. For others, it should be their top priority. Cybercriminals will strike when your organization is already in crisis mode. When they do, you must be able to defend yourself with limited time, attention, and resources. To do so, you must operate efficient, streamlined, semi-automated security systems.

In 2020, some organizations learned just how inefficient their security systems were. They struggled to perform simple daily security tasks and looked for outside help.

"Historically, my team is called when it's a really severe attack — something way beyond an organization's ability to respond with their in-house team," says McConkey. But since 2020, McConkey and his teams have been asked to help with far more mundane incidents.

"In many instances, we're called in because the organization's internal team is already swamped," says McConkey. "They're drowning in the alerts that are coming in because of all the new technology that's being deployed and additional changes to the IT environment. So, they have less capacity to field even small incidents."

When you can't handle even small, day-to-day responsibilities under normal circumstances, you'll really struggle to respond to a full-blown ransomware attack.

If this sounds familiar, be forewarned. When you can't handle even small, day-to-day responsibilities under normal circumstances, you'll really struggle to respond to a full-blown ransomware attack during a busy period. In that case, improving your security systems' efficiency must be a top priority.

Step Five: Re-evaluate your endpoint management and security tools.

Finally, take a look at your endpoint management and security tools. For each tool, ask yourself:

- Is this an isolated, single-function point solution?
- Does it require intensive manual labor to operate?
- In 2020, did this tool lose some or all of its ability to provide visibility and control?

Consider replacing any tool that receives one or more "yes" answers.

During a ransomware incident, any isolated, manual tool that delivers limited visibility and control will only slow you down, burden your teams, and increase your chances of having to pay.

"If you have thousands or tens of thousands of devices, you can't afford to have your team manually addressing each of them," Loura points out. "You need a well-instrumented platform you can use to gather data and run execution and action on a wide range of devices across the globe. An effective endpoint management solution is essential."

An effective endpoint solution like Tanium

How Tanium Can Help Secure Against High-Volume Attacks

Tanium delivers effective endpoint security under the harshest conditions. It provides a single, unified platform that offers a comprehensive suite of security capabilities.

Tanium employs a lightweight, distributed architecture that makes it quick to implement and efficient to operate.

Tanium employs a lightweight, distributed architecture that makes it quick to implement and efficient to operate. Tanium can be launched through a 100% cloud-based deployment that scales visibility, control and IT hygiene across rapidly evolving endpoint environments.

There are several reasons why security leaders, including those cited in this eBook, rely on Tanium to maintain effective security. In moments when their organizations are already engulfed by security and IT operations issues, Tanium:

- Delivers real-time visibility and remote control over expansive endpoint environments, making it easy to raise the barrier to entry into organizational networks and perform rapid, incident investigation, response, and attacker eviction.
- Provides a unified platform for core endpoint management and security capabilities, which allows security leaders to raise efficient, effective defenses without unnecessary complexity, cost, or team management challenges.
- Streamlines and automates many of the core tasks of endpoint security and management, making it possible to remediate complex threats in moments when technology resources are stretched thin.
- Can deploy new endpoint management and security capabilities in hours or days — not weeks or months — which allows security leaders to quickly spin up needed capabilities at a moment's notice.

The Tanium Platform offers critical services for combating ransomware and other cybercrime.

Asset Discovery and Inventory
Know what endpoints and applications are in the environment, even as the environment rapidly floods with new managed and unmanaged home-based agents.

Incident Response
Get an out-of-the-box, comprehensive suite of unified capabilities to rapidly detect, investigate, and remediate incidents without paying ransoms, which gives organizations a strong negotiating position against ransomware.

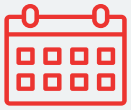
Data Risk and Privacy
Identify, categorize, and manage sensitive data in the environment to understand what an attacker might have touched and reduce the threat of data dumps within ransomware attacks.

Be Ready for Whatever Comes Next

It doesn't matter what vertical you operate in or whether you think your organization is a rich target. If your vertical has been overwhelmed by attacks, and your organization has the budget to pay a ransom, cybercriminals will target you when you feel least prepared to fight back.

When that day comes, will you be ready? You need to be **ready for whatever comes next**.

Reach out today to learn if Tanium can help secure your new environment and remain safe no matter what happens next. Take the appropriate next step to see if Tanium is the right platform to drive your ongoing security requirements.



Schedule a free consultation and demo of Tanium.

Schedule Now

Let Tanium perform a thorough gap assessment of your current capabilities.

Get Gap Assessment

Launch Tanium with our cloud-based offering, Tanium as a Service.

Try Now

TANIUM

Tanium offers an endpoint management and security platform built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.