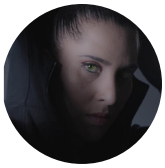

How Organizations Must Rethink Security in a Work From Home World

Advice From a Recovering Hacker

An interview with Alissa Knight, group CEO at Brier & Thorn, partner at Knight Ink and principal analyst

"It's the human condition to believe that we are prepared. But then when the thing actually happens, you realize how unprepared you actually were."

Alissa Knight watched the pandemic arrive.

She saw organizations struggle to maintain operations.

She realized these organizations were about to drop their guard.

She knew hackers would take advantage of the moment.

And she knew how to stop their attacks.

CYBER THREATS OPENED BY COVID-19

A Recovering Hacker's Perspective

Alissa Knight is a recovering hacker, serial entrepreneur, author, and thought leader. She currently acts as group CEO of the managed security service provider Brier & Thorn, a partner at Knight Ink, and as principal analyst at Alissa Knight & Associates.

Knight began hacking at 13 years old. She was caught hacking into a government network when she was 17. Released on a technicality, she later began working for the U.S. intelligence community supporting the cyber warfare directorate.

Since then, Knight has founded and sold multiple ventures in the cybersecurity space, started a venture capital fund, has published a book on hacking connected cars, and has continued to work hands-on within the cybersecurity field for the past twenty years.

When the pandemic struck, Knight guided many of her clients through the new security challenges opened up by COVID-19 and the mass mandate to Work From Home (WFH).

Knight knows the vulnerabilities that organizations now face. She understands how hackers are exploiting these vulnerabilities. And she has learned the steps organizations must take to defend themselves today and tomorrow—no matter what comes next.

Here is what Knight has learned.

A LOW BAR FOR ENTRY

COVID and WFH Open New Vulnerabilities

The pandemic struck. Businesses began to shut down. Workers were sent home.

Knight watched this, and began to worry.

“I realized that the bar of sophistication for adversaries was being lowered,” said Knight. “You have an entire economy of people now working from home who don't have a cyber-security budget for their home. The attack surface has increased exponentially, and has become a massive soft target.”

Knight saw multiple vulnerabilities open overnight.

More Targets

Organizations sent their entire workforces home. That included executives, system administrators, and others with privileged access to the corporate network. Adversaries suddenly had more high-profile individuals to target who could provide the "keys to the kingdom through elevated access privileges."

More Shadow IT

Organizations were not prepared to make this transition. They did not have enough bandwidth, VPN licenses, or laptops for their new remote workers. Their workers had to pick up whatever personal devices they had at home, and connect to the corporate assets through public networks.

More Backdoors

Organizations did not consider the other devices on these home networks—such as smart refrigerators, baby monitors, IP cameras, and gaming devices. Any of these could be compromised. Adversaries could then move laterally to the employee’s personal work device, compromise that, and then move to the corporate network over VPN split tunnels.

Less Security

Organizations did not extend their existing security controls to this new environment. Now, adversaries no longer needed to hack a hardened perimeter. They only needed to send a weaponized PDF to an individual working from home who lacked appropriate anti-virus, patching, or vulnerability management capabilities.

Knight saw these issues add up. They created a perfect storm of security vulnerabilities.

And she watched malicious actors immediately take advantage of it.

> “
>
> **History has taught us that attackers will always shift their attention to wherever there is a broader attack surface — wherever they can find the most victims.**

WHAT HACKERS WANT

Explaining the Malicious Mindset

As a “recovering hacker”, Knight understands her adversaries, and what they seek.

In part, they seek the thrill of the hack.

“It’s like a drug,” said Knight. “Knowing you can access anything, anywhere, anytime... you feel like a god—and you want more.”

In the past, hackers chased this feeling, and primarily sought recognition from other members of their community. They would mostly just compromise websites and tag them with digital graffiti that let everyone know who had pulled off the hack known as website defacements.

But times have changed, and attackers have adopted much more sinister motivations.

"It's now 20 years later, and it's no longer about defacing websites. It's about finding, stealing, and monetizing data," explained Knight. "That's the reason behind ransomware. That's the reason behind adversaries targeting organizations—they are looking for Personally Identifiable Information (PII), usernames and passwords, and payment card information that can be stolen, monetized, and sold on the black market."

In this sense, the pandemic has been a gold mine for these hackers.

It has created distributed operating environments that are filled with valuable data, and countless new ways to access it.

At the same time organizations were rushing to spin up these new environments, adversaries were rushing to find the best way to exploit them.

And many have been successful.

TODAY'S NEW ATTACKS

Exploiting the WFH Environment

Malicious actors have kept busy the last few months.

"I do a lot of incident response and forensics, and the number of IR engagements at Brier & Thorn have nearly doubled," said Knight. "I can attest to the news that the number of breaches have increased since the WFH economy started."

To create these new breaches, adversaries have not simply launched more attacks. They have adapted their methods to directly target the new WFH environment, through a combination of conventional social engineering and new types of malware developed to exploit Mac devices.

"History has taught us that attackers will always shift their attention to wherever there is a broader attack surface, wherever they can find the most victims," explained Knight. "With the new WFH economy, adversaries know they are going to run into more OSX devices, versus the Windows devices you typically see in an enterprise environment. They are going to adapt to that, and that's exactly what's happening."

> "It's no longer about defacing websites. It's about finding, stealing, and monetizing data...That's the reason behind adversaries targeting organizations—they are looking for Personally Identifiable Information (PII), usernames and passwords, and payment card information that can be stolen, monetized, and sold on the black market."

Since March, Knight has seen a rise in new crime kits, back doors, and command and control exploits for Macs and other mobile devices. To get these threats onto user devices, adversaries have been leveraging social engineering campaigns targeting those looking for employment.

> Too many breaches are the result of an attacker exploiting a vulnerability that has a patch available for it. Organizations are not patching fast enough. They need technical controls that enable them to identify vulnerabilities that need to be patched, and to apply those patches.

"What adversaries will do is called 'Hacking the Human' or social engineering," explained Knight. "They will target an individual at a specific company based on their title. They will talk with them, gain their confidence, create a relationship, and then send them a PDF. When that PDF is opened, it will execute malicious code, and create the backdoor on their system."

This backdoor will give the attacker access to anything they want on the victim's device. It might even give the attacker access to the corporate network.

Over the course of the pandemic, Knight has seen these attacks increase in their sophistication.

And yet, despite the rise in targeted attacks molding themselves to the unique contours of today's operating environments, Knight still feels the biggest threats to organizations today are much more fundamental problems that have become even more challenging during the pandemic.

VISIBILITY AND CONTROL

The Key Challenges Organizations Face Today

When asked about the biggest security problems organizations now face, Knight was clear.

"It's a dichotomy of visibility problems into the assets an organization has out there, and a lack of vulnerability and patch management on the endpoint," said Knight.

For Knight, resolving this fundamental problem begins with re-establishing visibility across the entire operating environment.

"The biggest threat to organizations today is not knowing about the assets that they've got," said Knight. "What we refer to as the Shadow IT problem. An employee deploying a server that has been unpatched, unsecured, unhardened into the network, and accessible from the internet."

The rapid move to WFH has flooded operational environments with these unknown assets.

"We need to know what assets we have, because organizations now have assets everywhere," said Knight. "And now organizations have more devices that historically weren't connected being connected and reachable from the Internet."

Knight knows first-hand how valuable these unknown assets can be to a hacker.

"Over the last two decades of my career, I've hacked over a hundred networks in penetration tests," said Knight. "More than half of those compromises were the result of me gaining access to the network through an asset the company didn't know they had."

For Knight, this lack of visibility feeds into the

second problem set crippling most organizations' ability to protect their new WFH environments—an inability to manage patches and vulnerabilities on the assets they know they have.

"Too many breaches are the result of an attacker exploiting a vulnerability that has a patch available for it," explained Knight. "Organizations are not patching fast enough. They need technical controls that enable them to identify vulnerabilities that need to be patched, and to apply those patches."

While Knight affirms that re-establishing visibility and control are the most important actions that organizations can take to secure their new environments, she also acknowledges there is no one "silver bullet", and that today's security challenges demand multiple, complex answers, that may force organizations to rethink their approach to how security is performed.

> "Over the last two decades of my career, I've hacked over a hundred networks. More than half of those compromises were the result of me gaining access to the network through an asset the company didn't know they had.

SECURING TODAY'S WFH ENVIRONMENTS

A New Narrative

Knight challenges many of the assumptions of her industry, and the security problems opened by the pandemic and the rapid transition to WFH appear to validate much of what she says.

Knight believes:

Centralization is Gone. "We need to get away from this idea of a central office and network. A lot of organizations are going to stay in a permanent WFH architecture. The perimeter is gone. And the new workforce of Millennials and Gen-Z workers want to work differently than previous generations. They want to work from anywhere, from any device, on their own hours. The idea of 9 to 5 and reporting into an office is a precept created during the first industrial revolution before knowledge work arrived in the 1950s. It simply doesn't work for the new workforce in today's economy."

Defense-in-Depth is Dead. "The idea of defense-in-depth is very much a castle-and-moat mentality. You had your crown jewels, which was the castle, and the moat was built around the castle to protect it. The problem is data is mobile. It's now in our employees' homes and we have no purview over it. We can't have the moat because data is everywhere."

Security Must Move to the Data. "We need to rethink data security. The idea that we know where data will be all the time to secure it as such is epistemically delusional and intellectually arrogant. We need to figure out what it is we're trying to protect, determine where it is, and then build security controls like layers of an onion around it. We need to secure data everywhere it lives, and everywhere it could go. Security should therefore travel with the data, not on the infrastructure we think it will never leave."

Prevention is No Longer Possible. "Nowadays organizations know it's not about if they are going to get hacked, but when. And the question is what security controls can you implement—on the network and on the endpoint—in

order to lower the amount of time it takes to detect them so you can eradicate them from the network."

Ultimately, Knight summarizes her perspective on how organizations must approach securing their operational environments—against today's threats, and against whatever tomorrow brings—through a simple sentiment, first made by Sun Tzu in the Art of War, that she summarizes.

"We can't bet on the enemy not coming, because the enemy will come. We simply need to make our position unassailable."

This interview is part of the interview series, When the World Stayed Home, which takes a comprehensive look into IT challenges that were exacerbated by the COVID-19 pandemic and how organizations are shoring up their weaknesses while preparing for the unknown future.

visit world-at-home.tanium.com

brought to you by Tanium