Gaining visibility to network attacks

While COVID-19 is exploding the size of corporate networks far beyond the firewall, CISOs are wrestling with limiting attack surface risk. Controlling endpoints and deploying zero trust models are key to containing potential breaches. Evan Schuman reports.

There is little debate that COVID-19 ushered in massive changes to the attack surface starting in March 2020. The most dramatic change was that almost all enterprises flipped staff from roughly 90 percent in-house and 10 percent external to 90 percent external and 10 percent inhouse; sometimes the work-from-home (WFH) percent reached 100 percent. That complete reorientation relates to both people as well as dataflows.

Added to that was a sharp increase in cloud usage — authorized as well as shadow IT — along with a massive increase in the use of internet of things (IoT) devices and untrusted networks, and CISOs soon found themselves looking at a threat landscape with a massively expanding attack surface spreading at speed over a very short interval of time.

The ongoing pandemic is wreaking havoc with pre-COVID-19 plans to reduce the networks' attack surface, experts agree, so new strategies are being developed to contain, rather than eliminate, the potential threats at the moment.

Among the security strategies that are being re-evaluated in light of the sea change of the forced digital transformation and relocation of users off the corporate network include:

- **Bring your own device (BYOD):** Many users now work from home and frequently use untrusted, unknown networks and personal devices for business use;
- **System information and event management (SIEM) systems:** SIEMs are designed to operate within the trusted firewalls and the corporate IT environment;
- **Virtual private networks (VPN):** Can have issues scaling to meet corporate requirements;
- **Greatly reduced on-premises network management for users:** A situation similar to the challenges of the SIEM in that it is not appropriate for remote users.

The work-from-home (WFH) trend begs the questions: Is on-prem management still on-prem if users are remote, working from untrusted networks, and no longer managed directly by an enterprise's security staff? When does the corporate network become little more than another private cloud?

Deconstructing the "new" network

There is even renewed debate about router ownership and control, given that the percentage of the attack surface controlled by such hardware is now so massive in that employees' home networks and functionally an untrusted component of the overall corporate network. The debate centers on

OUR EXPERTS: Threat surface

Azeem Aleem, VP Cybersecurity Consulting, NTT

Neil Daswani, co-director, Stanford University Advanced Computer Security Program; former CISO, Symantec

Brandon Hoffman, CISO, NetEnrich

David Holmes, senior analyst, Forrester

Phil Lieberman, independent security consultant

Greg Rattray, consultant/co-founder, Next Peak; former CISO, JPMorgan Chase; former director for cybersecurity, National Security Council

Tony Sharp, senior vice president, Booz Allen Hamilton

Steve Zalewski, deputy CISO, Levi's

Threat surface

65%

Anticipated percentage of the world's population that will have its personal data covered under new privacy regulations by 2023.

– Gartner

several key issues: the cost of purchasing and installing company-owned routers; the challenge of maintaining them; issues surrounding the user-to-service-provider issues for support on topics that might not impact the router directly; and what happens when an employee quits, moves or otherwise changes infrastructure and/or devices.

Of course, the dramatically larger and more dangerous attack surface caused by COVID-19 is being combatted with identical or smaller corporate security budgets, thanks to plunging revenue from cratering economies across the globe.

Where do CISOs start? According to several of the experts mentioned in this story, this might not be what anyone wants to hear: CISOs need to start at the beginning. They

Defending a growing attack surface

When enterprise environments flipped in March, moving from roughly 90 percent of employees inhouse to 90 percent external, the daily activity and the number of authorized personnel did not materially change, but the risk factor did. As cloud activity increased, internet of things accesses soared and remote connections increased exponentially, communications that were barely problematic last year morphed into something highly insecure.

"Attack surface is really just an extension of your organization's footprint into the public internet. Everything you strive to do internally should be done with more vigor outside, because it is more easily attacked," says NetEnrich CISO Brandon Hoffman, speaking during an SC Media webcast titled "Managing the attack surface."

"Additional considerations include contextualize threats, increasing identity and authentication requirements, consistently reviewing and removing unnecessary services, as well as weaving security into development and DevOps at every chance," he adds.

To deliver sufficient defenses, all activity must be monitored continually. That might sound obvious, but truly continuous monitoring is rarer than today's environments demand.

"We all know how dynamic the IT landscape inside companies are so testing in a static mode really does not provide a quality frame of reference to reduce risk. You generally don't need people to do the testing because there are tools out there that run automatically and provide output," Hoffman says. "That's where we need people. People that understand the output of the tool and can prioritize what action needs to be taken."

One of the advantages, and a key disadvantage, of enterprise threat intelligence is the massive volume, with most multi-billion-dollar companies leverage dozens of different of threat intelligence feeds, including verticals, geographies, open-source, government, industry and a variety of homegrown feeds based on security information and event management (SIEM) system output. That volume is a blessing when trying to use machine learning to make sense of the trends, but it is a curse when feeds contradict each other or distract security analysts with irrelevant data.

In today's new environment, these intel feeds pose new challenges and opportunities for the CISO.

"The tricky part of using threat intelligence for the attack surface again comes back to knowing what your organization has exposed externally. Generally speaking, the most important parts of threat intelligence as it relates to attack surface would be correlating methods that align with exposed services, certificate transparency logs, nefarious domain registrations and related records, and classic indicators of compromise to a degree," Hoffman says.

— ES

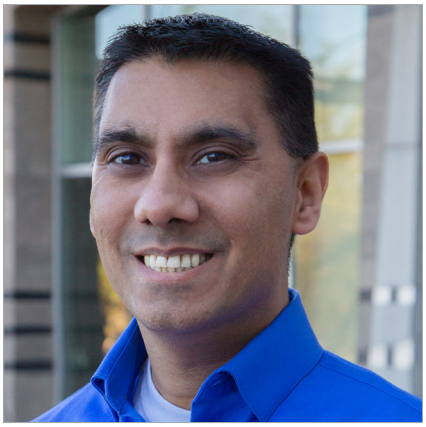
$7.1M

Average cost of a healthcare industry data breach is $7.13 million in 2020, 84% higher than the global average

– AksjeBloggen.com

need to take a step back and re-evaluate all elements of cybersecurity, given that so many of the processes, procedures and tools were designed to protect a massively different environment. And while CISOs are coming up with new environment-appropriate mechanisms, cyberthieves and well-financed state actors are thinking up new and better attack methods for the same environment.

Today it is not so much a matter of shrinking the attack surface as much as protecting this much larger attack surface. Once secured, the protected larger surface potentially brings tremendous benefits to the enterprise in terms of efficiency and productivity and recruiting.



Neil Daswani, co-director, Stanford University Advanced Computer Security Program; former CISO, Symantec

Many of our experts say tracking this space see this 90-to-10 flip as ultimately a good thing for security, in that it is forcing newer approaches, such as zero trust and continuous authentication and behavioral analytics, to the top of the To Do lists while traditional and entrenched approaches are being reconsidered.

"It turns out that the exodus of office workers during the pandemic has been the proving ground for zero trust," says David Holmes, senior analyst at Forrester Research Inc. in Cambridge, Mass. Many organizations were looking at a zero trust strategy before but the most common question these clients had was where to start. The pandemic forced them into a choice.

"They could either greatly expand their existing and often fragile VPN infrastructure, thereby increasing their threat surface, or adopt a zero trust access strategy with one of the many vendors who offer it as a cloud-based SaaS," he continues. "I advised dozens of these clients during the pandemic and, in the early days, about two-thirds chose the VPN option against my advice because it was a devil that they knew. But that other third was choosing [cloud offerings]. Cloud enabled those approaches to scale. Several vendors have told me that the number of users going through their systems increased by an order of magnitude — in one case, 13x — during the pandemic," he says.

Holmes argues that the 90-10 employee flip proves the need for zero trust without enterprises having had to make a conscious choice of taking on the risk.

"Conservative organizations, mid to late adopters, don't have to wait to see if zero trust is viable. The pandemic has proven it," Holmes continues. Citing author Geoffrey Moore's book *Crossing the Chasm* and his discussion on technology adoption lifecycle, Holmes notes, "You know that for a new technology, there's a chasm between the early adopters and the rest of market, and crossing that chasm is tricky for that community. In my entire career, I have never seen an externality like this pandemic that forced a whole market to jump that chasm overnight."

> "Unmaintained, not frequently used legacy systems attract the equivalent of digital cockroaches."
>
> *– Neil Daswani, co-director, Stanford University Advanced Computer Security Program; former CISO, Symantec*

Enterprise cloud growth — which is accelerating far faster year-over-year for 2020 than at any point in cloud's history —

Threat surface

12%

Survey says only 12% of CISOs are considered "Highly Effective"

– 2020 Gartner CISO Effectiveness Survey

is another area where Holmes sees major changes.

"The pandemic has also accelerated another trend: The migration of the traditional security stack not to the cloud itself, but to global edge networks. The thick edges have become safer on-ramps to the internet and allow organizations to basically outsource network security and access to a third party," Holmes says. "In this model, a firewall gets consumed as service, just like malware analysis and CASB. Forrester calls this model a zero trust edge because it uses zero trust access for all the remote users, too."

Phil Lieberman, independent security consultant

Digital cockroaches

Phil Lieberman, a security consultant, sees the better-managed cloud sites as deliver far better security when compared with almost everything else in an enterprise environment.

"CIOs and CISOs have an easy time managing and securing commercial cloud software like Salesforce, Office365, SAP, and other single-vendor approaches," he says. "The cloud vendors themselves maintain the security of the stack of these products. The only hard part is getting the identity, privilege, and access management correct. There are plenty of vendors and guidance for commercial software packages."

Lieberman continues, "The same rich ecosystem of secure stacks and commercial management does not exist in the mishmash of in-house and cloud frameworks, microservices, and component application stacks."

A long-problematic area for enterprise environments has been legacy systems, which even the huge changes from the 90-10 split are not going to resolve.

"Unmaintained, not frequently used legacy systems attract the equivalent of digital cockroaches," says Neil Daswani, co-director, Stanford University's Advanced Computer Security Program. "Often better to shut them down to reduce the attack surface than try to maintain them via patching, sandboxing, firewalling, [and the like]."

One critical consideration with these environments is that they are not merely much larger, but they are far more complex than what enterprises dealt with last year. And new complexities initially bring new security holes.

Greg Rattray was CISO of JPMorgan Chase until June 2019 and earlier served on the National Security Council as director for cybersecurity in the George W. Bush administration. Currently he is a cybersecurity consultant and the co-founder and partner of New York-based Next Peak. He sees this new complexity as a concern.

> "Some SIEMs don't do well with a messy data lake. Discipline is needed in what is coming at the SIEM."
>
> *– Greg Rattray, consultant/co-founder, Next Peak; former CISO, JPMorgan Chase; former director for cybersecurity, National Security Council*

"The current pace of technological change and the necessity of accommodating remote work has resulted in a growing number of devices, operating systems and data streams for most enterprises. The real issue with this lies in the volume and complexity of security data. The data created by monitoring expanded attack surfaces creates large,

71%

Percentage of organizations that report issues with native security provides provided with cloud-delivered email offerings

– ESG

unfiltered data streams and lakes that when processed by security tools results in false positives," Rattray says.

"This situation makes it difficult to find real threats while also costing companies money," he continues. "Reducing and filtering the flow of data to your security operations can provide clear optics of your attack surface which will help with identifying real malicious activity. With data discipline, your attack surface may continue to grow, but security teams can improve their ability to see and stop attacks more accurately and efficiently."

Azeem Aleem, VP Cybersecurity Consulting, NTT

Doesn't SIEM like old times

Rattray extends that argument to the most basic elements of must enterprise security environments, starting with future of SIEMs. "Some SIEMs don't do well with a messy data lake. Discipline is needed in what is coming at the SIEM," he said, noting that sometimes "you pay for the amount of data that is being processed" with some and that CISOs must "put energy into knowing what data is coming at you. Be disciplined what you put into it. You can make [your SIEM] smarter."

> "Moving from a reactive to a proactive and predictive strategy using threat intelligence is the way forward. To do this, you need full visibility to detect threat patterns."
>
> *-Azeem Aleem, VP Cybersecurity Consulting, NTT*

Stanford's Daswani shares some of Rattray's SIEM concerns. "SIEMs collect logs and data from tons of devices on the network. Are SIEMs still useful? Yes, but perhaps not as useful as before. But that doesn't mean that they can't be made just as useful again," Daswani says, adding that the logs of all of these new endpoints need to be aggressively fed into the SIEM.

Azeem Aleem, vice president of cybersecurity consulting, global digital forensics and incident response lead for NTT Ltd. in the United Kingdom, bluntly says "SIEM has no future. Organizations lack visibility and are still relying on tools like SIEM for advanced monitoring, which can only detect about one percent of advanced attacks. The traditional prevention approach has become a failed strategy. You will be breached," he says.

"Moving from a reactive to a proactive and predictive strategy using threat intelligence is the way forward," Aleem says. "To do this, you need full visibility to detect threat patterns."

Aleem says a lot of today's more advanced attack vectors simply bypass the SIEM, forcing a more rapid transition to behavioral analytics.

Another security consultant, Tony Sharp, senior vice president at Booz Allen Hamilton, is also pessimistic about SIEM's future.

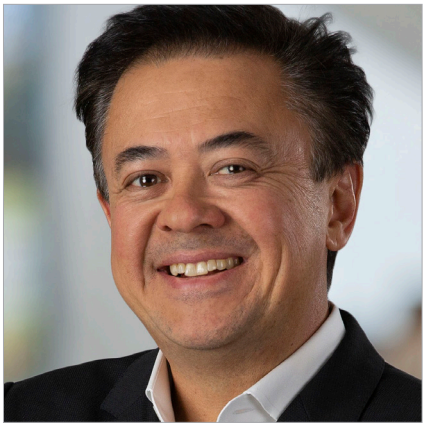
SIEM will not survive in its current construct, he says. Evolution is required here given the shifts in technical architectures that will persist, such as cloud native, edge compute, and other technologies. "This becomes a big data management and visibility matter, where trained ML (machine learning) models working as inputs into AI-generated (artificial intelligence) response actions to adaptive NGEN (next generation) SIEM playbooks become a reality of security operations."

$3.7M

The average global cost of a data breach is $3.86 million, down 1.5% from 2019

– Ponemon Institute's Cost of a Data Breach Report 2020

The deputy CISO for San Francisco-based apparel giant Levi's, Steve Zalewski, is also concerned about the future of SIEMs but he has much bigger worries. "The SIEM traditionally is about protecting your systems and your assets, but most of my endpoints are now remote. How do I re-spin my SIEM now?" Zalewski asked. "We still have VPNs but we're getting away from that."



David Holmes, senior analyst, Forrester

Zalewski's core concern involves the dataflow and how people work. There are three modes of workstyle/dataflow that Levi's has: a major corporate office/campus; telecommuting; and road warrior. COVID didn't merely all-but-wipe-out corporate locations, but it also obliterated road warrior travel.

"Now they can't travel and they can't go into the office. When people are out of their comfort zone, that's when mistakes happen," Zalewski says.

> "How does [owning and managing my employees' routers] help me sell jeans? For the cost of trying to do that, is there an ROI there? [especially given that] the place where I most need it – Asia – is the place where it's hardest to do."
>
> *–Steve Zalewski, deputy CISO, Levi's*

Managing home routers

A long-debated topic within IT and security is router control. In theory, it would sharply decrease security complexities if all routers were of the same type and brand and they were maintained on a constant schedule maintained by centralized IT talent. Patch management is just one example of the kind of generic IT control home-based employees' routers that is considered an essential task.

Before March, the answer almost always was "No, given that home routers control such a small slice of our traffic, centralized ownership would not improve the enterprise risk profile sufficiently to be worth the cost and effort."

Since March, however, the discussions have renewed, given that employee-owned routers now contribute such a huge portion of enterprise risk. Then again, the costs of such ownership have increased sharply, as the number of routers needed has increased.

Although multiple security experts say router ownership merits serious consideration today, Levi's deputy CISO is not among them, at least when it comes to Levi's systems. The reason for that has less to do with risk or cost and more with global concerns.

Given that Levi's does business in more than 100 countries, Zalewski says, the complexities involved in such ownership are not only extreme, but it is impossible to have one brand globally, no matter what.

"I can't use the same routers. In Russia, routers can only be purchased from within Russia. The same thing for China," Zalewski said, adding that Levi's also operates in geographies where dialup connections are still used. "There's so much variability that I'd have to break it up in regions. You have to allow the regions to use whatever technology is available."

Even for those countries where consolidated router ownership was possible, Zalewski said, it would still come down to money and it would likely be a losing argument. "How does [owning and managing my employees' routers] help me sell jeans? For the cost of

57%

Percentage of WFH knowledge workers who say the pandemic showed they can work from home effectively and want to do so in the future

– ESG

trying to do that, is there an ROI there? [especially given that] the place where I most need it — Asia — is the place where it's hardest to do."

Another critical concern with the new environments is browser protections. Stanford's Daswani is a strong proponent of air-gapped browsers, where all browsers "would run offsite in a hardened environment and [users] would rely on the browsers just for display."

Forrester's Holmes says browsers are part of one of the most fundamental environment changes.

"Your current network monitoring practices won't work anymore. Two of the foundational protocols of the internet, transport layer security and DNS, have recently undergone radical changes to protect browser user privacy. Both changes have created controversy in the security community because, although they hide user activity from the searching eyes of nation-states and ISPs, they also hide valuable metadata from enterprise network inspection tools," Holmes says.

"As these changes gain momentum, security monitoring tools will be blind to the content and destination of traffic and unable to detect threats," he concludes. "The network will be darker than it's ever been." ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at (347) 480-1749, or via email at david.steifman@cyberriskalliance.com.

Threat surface

1 dead

A patient at Huessendorf Hosptal in Germany died after a cyberattack shut down 30 servers and emergency room equipment

– The Guardian