




THREAT MATRIX 2018: IS YOUR COMPANY PREPARED FOR SECURITY RISKS EMERGING IN THE COMING YEAR?



ACADIA



TECHNOLOGY GROUP



CIOs face the unenviable task of holding back the tide of network security threats sweeping the globe. It seems the traditional approach to protecting data is inadequate in the face of sophisticated attacks like the ransomware campaigns and phishing attacks.

Firms that are alert and serious about protecting the integrity of their data networks find themselves outmatched against the new wave of organized crime targeting them. The focus of this document is to reveal key ways enterprises and commercial organizations of all sizes can leverage new, innovative tools for lessening the damage a network security breach can cause.



A LOOK BACK AT 2017:
SECURITY BREACHES FROM
WANNACRY TO EQUIFAX

A LOOK BACK AT 2017: SECURITY BREACHES FROM WANNACRY TO EQUIFAX

CIOs face the unenviable task of holding back the tide of network security threats sweeping the globe. It seems the traditional approach to protecting data is inadequate in the face of sophisticated attacks like the ransomware campaigns and phishing attacks.

2017 turned out to be a year filled with some of the most massive breaches of corporate network security of our time. To truly understand the innovations we'll reveal later on, it's important to have a clear view of the threat landscape and gain a firm understanding of how we've reached the current security threat levels in the face of seemingly non-stop attacks on corporate networks.

WANNACRY: AN ALMOST PERFECT STORM OF RANSOMWARE ATTACKS

May 2017's WannaCry threat stretched across the globe, rocking the core of Spain's main telecommunications provider Telefonica and the U.K.'s national health program; preventing patients from receiving critical care because of major lockdowns in the system. The nature of the attack was disturbing on many levels for those charged with keeping corporate networks and customer data safe.

It exploited a simple patch in the Windows operating system, demonstrating the struggle many organizations experience trying to keep up with patch management throughout their diverse environments. Firms with a solid control of their patching programs were fine while others, that preferred to not instantly install operating system patches due to security and predictability considerations were left vulnerable.

Trend: Aggressive network attacks have taken decision making out of the hands of C-level leadership in organizations, placing it squarely in the hands of bad actors looking to exploit even the simplest vulnerability.

How to Adjust: Network security leaders would do well to think like the bad actors to prevent infiltration into their systems. For bad actors, the current line of thinking is to find a small vulnerability in a network, exploit it and then lock down as many areas of the network as quickly as possible. With that in mind, corporate tech leaders need to explore ways to isolate attacks at the point of entry.

VAULT7: WIKILEAKS CIA BREACH AND BYOD SECURITY BREACHES

A few months before WannaCry, WikiLeaks released several CIA documents which revealed unique ways the U.S. government exploits vulnerabilities in mobile devices to listen in on the conversations of its citizens. The importance of these revelations can't be underestimated when reviewing the security landscape of 2017 and how it will affect the future of networks for years to come.

The leak shows just how easy it is to use mobile phones as listening devices. BYOD continues to grow in popularity and many firms have been forced to create policies around it. According to a recent study by Crowd Research Partners, 20 percent of businesses have suffered a security breach that originated from a mobile device.¹

20% of businesses have suffered a security breach that originated from a mobile device.

-Crowd Research Partners

Some would say no greater threat exists to corporate networks than an inexpensive smartphone an employee uses to access the corporate network, opening the door to a company-wide breach.

Trend: BYOD grows in popularity, dominating corporate networks and exposing them to unprecedented risk.

How to adjust: Devote a portion of corporate security budgets to endpoint security, improve segmentation and real-time detection capabilities, and take a future-forward approach to network security design and threat avoidance.

¹ Crowd Research Partners, "BYOD & Mobile Security Report," September 2017

EQUIFAX AND THE RISK OF IGNORING THE 'WHEN NOT IF' WAY OF THINKING

In September 2017 Equifax, one of the three major credit bureaus in the U.S. admitted that 143 million records containing consumer's personal information had been stolen from its network by cybercriminals.²

143 million records containing consumer's personal information had been stolen from its network by cybercriminals.

- Crowd Research Partners

This made global news because of the scope of the breach and the sensitivity of the information (social security numbers, addresses, birth dates, etc.) to which the thieves had access.

The popular lesson from this issue was to respond quickly to inform those affected of any breaches, but the real lesson is more about the mindset of the corporate technology leader. Leaders learned that they need to develop a "when not if" mindset with regard to security breaches. They learned that breaches **will** happen and sooner rather than later. Savvy, responsible organizations must plan not only for technological security controls and the incident response approach to a breach but also the public relations side of managing the fallout.

Trend: Corporations brace for public shaming and damage to their reputations stemming from the exposure of sensitive data while embracing the inevitability of the occurrence of breaches.

How to adjust: Develop an isolation strategy and data recovery contingency plan.

² Krebs on Security, "Breach at Equifax May Affect 143 Million Americans," September 2017

RISKS AND REWARD OF CLOUD COMPUTING: DOW JONES & COMPANY

Cloud computing provides amazing benefits to expand access and storage of critical data for corporations worldwide, but the groundbreaking technology's Achilles heel has always been security vulnerabilities. While many still take advantage of its many benefits and keep the security risks at bay as best they can, the cloud remains a glaring vulnerability for corporate networks. It also brings up discussions as to whether public, private, or hybrid cloud configurations are the best data storage option for organizations.

One major firm faced this dilemma by choosing a public cloud option and was rewarded with the exposure of the personal and financial records of more than 4.4 million of its subscribers. Dow Jones and Company, used an AWS cloud portal to give subscribers of the Wall Street Journal and Barron's access to their account information.³ The exposure was due to a configuration error that gave all AWS account holders access to the repository of private client information. Security team UpGuard found the vulnerability on June 1 and Dow Jones closed it on June 6.

Whether or not bad actors captured any information before the issue was addressed remains unknown.

Trend: Cloud computing remains a valuable tool in the CIO's arsenal, but bad actors know this and will continue to exploit any vulnerabilities in a cloud computing solution.

How to adjust: Implement the robust cloud security controls and configuration capabilities available through the provider to create a strong, isolated, and segmented security solution around your sensitive information. Act quickly to close loopholes, vulnerabilities, and openings cybercriminals could possibly exploit to access critical data.

³ UpGuard, "Cloud Leak: WSJ Parent Company Dow Jones Exposed Customer Data," November 2017

A LOOK FORWARD TO 2018: TRENDS IN NETWORK SECURITY THREATS

With an understanding of last year's breaches and the trends they've exposed, it's now important to take a look at what the coming year may hold and prepare by developing strong action plans for network/data security.

The conversation around network security inevitably turns to ransomware as it's been the major culprit of breaches over the past two years. At least three forms of technology present viable threats vectors to corporate networks and should be factored into any strategy for combating breaches.

WHERE SECURITY EXPERTS SEE THE THREAT MATRIX DEVELOPING IN 2018

THREE AREAS EMERGE AS THE BIGGEST THREATS FOR 2018. THEY INCLUDE:

BYOD and disappearing network perimeters:

Some research posits 80% of breaches originate from within the network perimeter.⁴ This calls to question the origin of attacks and brings up the issue of BYOD as a major source of network vulnerability which shouldn't be overlooked.

With the advent of BYOD, cloud computing, and wireless network access, the network perimeter shifts so much it's hard to know where or whether it exists at all. To secure such a moving target seems nearly impossible. The key is to accept that the idea "perimeters" may be obsolete and that the focus of diligent CIOs is to secure network data itself and not necessarily the perimeter that separates the outside world from said data. The aforementioned means automating security protocols, such as provisioning network access and limiting it to certain users so that security shifts quickly and dynamically as users interact with the network.

IoT and the expansion of end-point vulnerabilities:

IoT for enterprises promises even more efficiency and lower operating expenses, but one of the largest DDoS attacks originated from exploiting weak native security of IoT-enabled devices. Granted, these devices were consumer-centric, but the vulnerability inherent in network-enabled systems and devices comes from an expansion of end-point devices connecting to the network. With that expansion comes more risk. IoT devices will be the source of an exponentially expanding footprint of endpoints for enterprises, which makes it imperative for CIOs to make security and architecture best practices the primary concern when adding IoT technology to their organizations.

Ransomware's prominent foothold in the threat matrix comes from its dependence on phishing emails to enter and compromise networks.⁵ Since email remains and will continue to be a pillar of operations, the threat from ransomware persists and will continue to do so for the foreseeable future. Research shows attacks have increased but ransom payments have decreased. It's important to note that ransomware attacks are now more sophisticated and data isn't always released once the ransom is paid. This increases the effectiveness of the crime and forces enterprises to focus even more resources on isolating breaches so they don't affect the entirety of the network's assets.

⁴ ZK Research, "Evolve the Network into a Security Sensor and Enforcer to Improve Business Security," 2016

⁵ McAfee, "McAfee Labs 2018 Threats Predictions Report," November 2017

THE AREAS OF EASY EXPLOITATION FOR BAD ACTORS

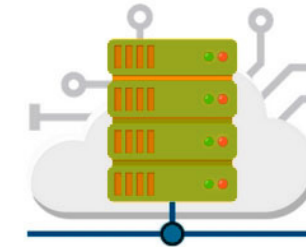
ONE OF THE BEST WAYS TO SECURE THE NETWORK IS TO ELIMINATE LOW-HANGING FRUIT AND ENFORCE SIMPLE BEST PRACTICES. AREAS OF EASY EXPLOITATION OF NETWORK WEAKNESSES INCLUDE:



EMAIL: Phishing attacks leveraging a simple misspelling of a company's domain name in the 'From' field have given cybercriminals access to entire corporate networks and the firms' most sensitive data. Data shows that no one is immune; top executives have exposed their companies to ransomware attacks by clicking on phishing email links. Along with dedicated and policy-based endpoint security, it's a best practice to issue reminders to all users on a regular basis to remain diligent and alert around this threat.



WiFi: Many businesses open their networks by allowing guest users access to their WiFi network. In the retail and the hospitality industry, allowing customers or guests access to "free" WiFi can be a driver of business (i.e., in-browser advertising, links to merchandise, discount codes). However, offering guest access through WiFi provides bad actors a way to potentially enter more sensitive areas of a network and compromise it. Some firms have found throttling their signal provides some level of security, but this approach does not resolve the underlying issue/vulnerability. Implementing automated role-based access to an Internet-only network segmentation for guests significantly reduces exposure.







CLOUD: Running applications on public cloud services remains a popular, but risky, activity for many enterprises. These risks are due, primarily, to application vulnerabilities that may be coded into the software itself. Without direct control over those applications, it's difficult for enterprises to protect their data. Best Practices in this area includes proper cloud architecture, implementing provider security and network controls plus SDN (Software Defined Networking) to manage and group devices as they come on and off the network.

HOW CYBERCRIMINALS EXPLOIT NETWORKS IN UNIQUE WAYS TO SPREAD MAYHEM

To protect a network against attacks it's important to understand who orchestrates the attacks and the systems they use to do it. Cybercriminals have become more business-like and sophisticated. A pattern emerges when looking at the characteristics of the most effective breaches.

Cybercriminals attack networks in four steps according to researchers from MIT's Sloan Management Review.⁶

-  **1 – Identify vulnerabilities.** It's important to note cybercriminals are constantly evaluating specific networks with designs on breaching them at some point. CIOs live with several sets of eyes on their backs because hackers play a game of cat-and-mouse looking for small footholds that they can expand into full-on breaches. No abnormality in network performance can be overlooked by those diligent about securing networks. The abnormality could be a cybercriminal in the initial stages of planning and executing an attack on the network
-  **2 – Expand and test.** Once the attacker gains a foothold in the network, some sources say they will review and explore the network for an average of three months before launching an attack. Here, CIOs have an opportunity to stop or isolate an attack before the real damage begins. Note this benchmark: The average time it takes a firm to detect an intrusion is 99 days.
-  **3 – Gain access.** Once the cybercriminal accesses sensitive data or the areas around that data, the clock speeds up. They know their breach is effective and they need only bide their time and look for opportunities to identify and exploit the firm's most important information.
-  **4 – Maintain access.** In this final stage, the attacker has compromised the network and can leverage that access against the target firm. It's in this stage the attacker locks down network access, exfiltrate data, and begins ransomware demands.

⁶ Heimdal Security, "MIT's Sloan Management Review: To Improve CyberSecurity, Think Like a Hacker," March 2017

USUAL REACTIONS TO NETWORK BREACHES

Following on the 'when, not if' mindset for CIOs, knowing how to react to a breach when it happens is also a best practice for enterprises serious about securing their networks. When companies experience a breach, a number of things happen including but not limited to:

Media firestorm/scandal: Media attention here depends on the profile of the company, recent and similar breaches or attacks, the amount of money or type of data loss, and a host of other variables. The key here is to communicate clearly with internal stakeholders about the breach, initiate a plan of action for controlling the message and notifying any external parties affected by the breach.

Financial blowback: Firms now purchase breach insurance to protect company assets and to provide restitution in the event of a breach of customers' financial and/or personal data. This insurance is often predicated on the assumption that the breach was not caused by corporate negligence or malfeasance.

Firings/re-organization: One of the more unfortunate results of a network breach is firings. Firings often set an example and distance a company from media intensity and the ire of those harmed by the breach. This shows tech professionals how high the stakes are in this area and how important it is to allocate funds, and both external and internal resources to shore up networks with the latest and best-of-class protective measures. Firings, as a result of a failure of upper management to listen to those responsible for maintaining security, can also damage a company's reputation as a good place to work. This impinges on the company's ability to hire top talent.

Re-structuring of networks: Developing a better network structure and putting more engineers to work on the network is a popular response post-breach. Keep in mind this can be a temporary fix and doesn't always address the full picture when one takes into account the potential for future breaches.

Development of new anti-phishing policies and procedures: Many firms strive to employ better endpoint controls, better ingress and egress controls and better email filtering to remove human error from the problem. In addition to this, many firms implement stronger, more comprehensive training programs for their companies, teaching employees how to properly identify and report potential or existing breaches. They also educate their employees about social engineering to ensure that the employees are aware security breaches often begin from seemingly harmless interactions in real life.



AN ELEGANT SOLUTION TO
A THORNY, ENDURING
CHALLENGE





AN ELEGANT SOLUTION TO A THORNY, ENDURING CHALLENGE

A dream scenario for many CIOs is to isolate and neutralize an attack at its point of entry, stopping it from ever entering the critical areas of the network. With software-defined networking (SDN), that scenario isn't a dream anymore. Leveraging this technology, firms can now identify, isolate, and neutralize breaches at the point of attack thus protecting the network and controlling data from one central location.

SDN FOR NETWORK PROTECTION

SD-Access, Cisco's offering of an Enterprise SDN solution, is software-defined networking for organizations looking to improve security, reduce operating expenditures, improve compliance and optimize the user experience. SD-Access allows administrators to design the network, provision networking gear programmatically and enforce group-based policies to secure the network. This opens up a world of opportunity not only for managing networks but for securing them.

As enterprises adopt new technology and embrace digital transformation, the number of endpoints connecting to the network will expand beyond the organization's capacity to manage them under the traditional network architecture. SD-Access gives CIOs the opportunity to have full control over how all IoT devices access the network, securing internal systems and isolating potential breaches before they have a chance to do major damage.

USE CASES IN NETWORK SECURITY WITH SD-ACCESS

SD-Access complements existing security solutions. Using role-based access control, white-listed users and devices can only access applications and resources they are explicitly given permission to access. This significantly reduces the impact of ransomware and malware attacks on the network.

Firms can now manage IoT devices efficiently without manual configurations that expose the network to inevitable human errors. It only takes one misconfiguration to cause an outage that jeopardizes business operations and, by extension, profitability.

SD-Access automates configurations based on the software-defined protocols set in place long before a device comes near the network. It's a strategic approach that puts network security and management on autopilot; almost completely eliminating human error and opening up a world of possibility for firms to embrace the growth that comes with adding applications and IoT-enabled devices to the network.

USE CASE	DETAILS	BENEFITS
Security and Segmentation	Onboard users with 802.1X, Active Directory, and static authentication <ul style="list-style-type: none"> ● Group users with Cisco TrustSec (Security Group Tags) and use group-based policies to control network access ● Automate VRF configuration (lines of business, departments, etc.) ● Traffic analysis using AVC and NetFlow is further enhanced using Encrypted Traffic Analytics (ETA) 	Faster, consistent and more efficient provisioning of network segmentation and user groups <ul style="list-style-type: none"> ● Limit the impact of breaches and prevent the movement of threats and compromised devices across your network with micro-segmentation
IoT Integration	<ul style="list-style-type: none"> ● Single point of definition for wired and wireless users ● Seamless roaming between wired and wireless ● Distributed data plane for wireless access ● Simplified guest provisioning for wired and wireless 	Management of wired and wireless networks and users from a single interface (Cisco DNA Center) <ul style="list-style-type: none"> ● Ability to offload wireless data path to network switches (reduce load on controller) ● Scalable fabric-enabled wireless with seamless roaming across campus
Cloud/Data Center Integration	<ul style="list-style-type: none"> ● Identity federation allows exchange of identity between campus and data center policy controllers 	Administrator can define user-to-application access policy from a single interface <ul style="list-style-type: none"> ● End-to-end policy management for the enterprise ● Identity-based policy enforcement for optimized ACL utilization ● Flexibility when enforcing policy at campus or data center

Source: "Cisco Software Defined Access Overview"

THE COST OF SD-ACCESS

One consideration here is cost. Implementing SD-Access requires upgraded network hardware, in particular, network switches. Organizations looking to implement any SDN solution will need to budget for hardware upgrades so that they successfully meet their objectives. The cost of implementing SD-Access is offset by cost savings in both in-house and outsourced IT operations.

The returns on this investment are additional network security and savings in time and money.

SD-Access allows the control of East-West traffic in the network with the use of policy-based forwarding decisions. This reduces any-to-any communications inherent in traditional network segmentation. Access policies are streamlined and presented in a user-friendly graphical interface, making management of security policies intuitive.

Deploying new network devices takes minutes instead of hours or days as network engineers and architects no longer need to manually configure network equipment. With Assurance and Analytics, administrators can monitor the health of the network, view device and application performance metrics, and proactively address issues increasing availability and improving the user experience.

Automating current IT operations frees up network administrators and architects to focus on strategic growth initiatives within enterprises and designing technological advancements that have a true impact on an organization's bottom line.

INDUSTRY-SPECIFIC COMPLIANCE ISSUES

Industries most likely to benefit from SD-Access include retail and healthcare because of the need to remain compliant with PCI and HIPAA standards. The stringent measures governing the use of credit cards and the handling of personal health information requires consistency in network policies and deployment.

In these cases, securing data means implementing an iron-clad, end-to-end segmentation that keeps traffic from users, devices, and applications separate. With SD-Access, engineers can handle these requirements without redesigning the network architecture and in a fraction of the time it would normally take to do so.



NEXT STEPS IN SDA ADOPTION ACROSS THE ENTERPRISE IN VARIOUS OTHER INDUSTRY SEGMENTS

Organizations looking to embrace SD-Access would do well to take a five-step approach to begin their journey. These steps include:

- Assess the existing hardware infrastructure, especially switches, and budget for replacements accordingly.
- Review existing 'inside the perimeter' security solutions. (Are existing security rules and access-lists documented? How are they updated as changes are made to the network?)
- Track the time it currently takes to configure networks, segment traffic, and redesign networks.
- Identify areas and lines of business that would benefit the most from SDN.
- Reach out to a trusted Cisco partner who can guide you through the finer points of integrating SD-Access into your network operations.



Premier
Partner

Acadia Technology Group is proud to be a Cisco Premier Partner, offering a full portfolio of solutions and services, powered by Cisco's leading technologies. We carry Cisco's spirit for innovation in everything we do, providing custom solutions for businesses with a wide variety of needs across a broad range of industries.

CONTACT US TO LEARN HOW WE CAN HELP YOU IMPLEMENT SD-ACCESS



973-233-1260



www.acadiatech.com



info@acadiatech.com



ACADIA



TECHNOLOGY GROUP