SKYBOX SECURITY

TEAR UP THE CYBERSECURITY RULE BOOK

Pioneer a new approach to vulnerability management

RESEARCH REPORT

GROWTH IN VULNERABILITIES IS A LEADING INDICATOR FOR FUTURE ATTACKS

Cybersecurity has become more complex than ever and current vulnerability management practices are simply not working. Already contending with a deepening skills crisis and the pressures of securing an ever-expanding attack surface, CISOs have now been forced to critically and fundamentally rethink their approach to security. Under intense time pressure, the CISO worked alongside the CIO to enable and secure their distributed workforce — a move that expanded the attack surface and introduced new risk.

CISOs are now taking stock of everything that has taken place over the year. After making it through the first wave of changes, they are establishing how well prepared they are to handle risk and determining just how much their attack surface has expanded. Many have reached the conclusion that they need to restructure their security programs, at least in part.

Long-held strategies that previously helped manage increased risk are no longer working this new security landscape. The World Health Organization reported a five-fold increase in cyber attacks since the onset of the Covid-19 pandemic. At the same time, security teams' existing workloads are growing in volume as new technologies and services are introduced. And the cybersecurity skills crisis is deepening:

45% **of security and IT professionals** believe that skills shortage has gotten worse over the past year[1].

Further, macroeconomic pressures are making it paramount that CISOs demonstrate the business value of their investments such as gaining efficiencies and reducing risk.

While necessity may be the mother of invention, the chaos that this year has brought could be the most pivotal time for the security industry. 2021 is poised to be the year that organizations remove the guesswork from security. This will require a shift in mindset away from traditional, antiqued remediation approaches toward modern, insight-driven security programs.

1 The Life and Times of Cybersecurity Professionals, ISSA, 2020

VULNERABILITY MANAGEMENT PRACTICES HAVE NOT KEPT PACE WITH CHANGING SECURITY LANDSCAPE

The growth in vulnerabilities is a leading indicator for future attacks. And the number of attacks are increasing exponentially every year. Simply put, enterprises are not going to be able to stop the increasing number of ransomware attacks, which are exploiting the growing number of vulnerabilities. To make things worse, the amount of vulnerabilities are expanding across multiple different types of software and different devices. To boot, vulnerabilities in OT networks are impacting IT networks in a more significant way.

Why are we in this situation? Currently there is an over-reliance on scanning and patching; security practitioners are assuming that what they are doing is good enough. There are an increasing number of vendors and point solutions, with the average enterprise using 75 security products to secure their network[2]. This leads to inconsistent volumes of disparate data sets, incomplete analysis, and fragmented internal processes. Enterprises are not able to prioritize vulnerabilities with the necessary granularity, and therefore are not addressing the greatest risk. There is poor understanding of network security controls relative to the huge volume of assets. And there are limited remediation options to address the exponential increase in vulnerabilities.

The average Enterprise uses **75** security products to secure their network

Enterprises can't keep up with the pace

New vulnerabilities are projected to exceed 20,000 in 2020 (this is up from 6,000 in 2016); this is a leading indicator for future attacks

Enterprises are unable to stop greatest risks to the organization

New ransomware samples are up 72% in 1H 2020 and are exploiting multiple vulnerabilities

New vulnerabilities are expanding across multiple OS, SW, device types

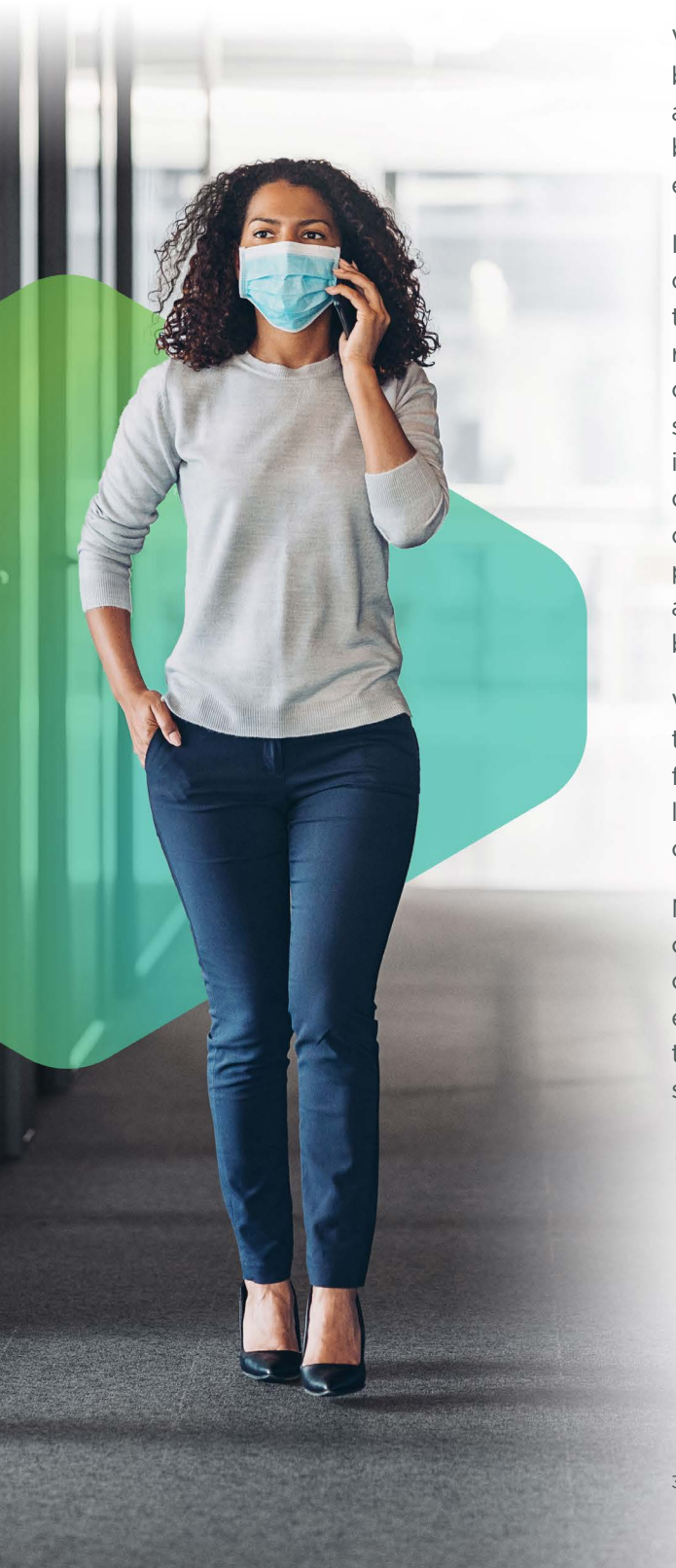
including: Android, Windows, Chrome, OS X, iOS, Edge Chromium, iPodOS, RedHat OpenShift, IBM API Connect, Oracle E-Business Suite

Convergence of technologies is increasing risk

Vulnerabilities in OT Networks are impacting IT Networks; OT Advisories are up 16% in 1H 2020

2 CSO, "Defense in depth: stop spending, start consolidating" 2016

A NEW PARADIGM: FROM DETECT-AND-RESPOND TO PRESCRIBE AND PREVENT



While many organizations invest millions in security controls to block, detect, prevent or respond to attacks, their vulnerabilities and misconfigurations in all layers of their environments are being exploited routinely, leaving organizations chronically exposed to material cybersecurity and compliance risks.

It is not practical or advisable for security organizations to continue investing in point products to paper over the cracks in their environment. This was a realization that many CISOs had reached before the onset of the pandemic, and they started to consolidate security vendors and tools. In 2019, 63 percent of security leaders cited 10 or fewer vendors in their environment in comparison to 54 percent two years prior[3]. Considering how different the security landscape is this year, it is likely that consolidation will accelerate. Instead of investing in point products to tackle specific problems within siloed security areas, it is now time to consider how any new procurement can benefit the security program as a whole.

With expanded responsibilities and workloads, an increased threat profile, and pressure to prevent the possibility of falling foul to regulatory fines or suffering data compromise, security leaders need a holistic approach that provides intelligence and context to make informed decisions.

New best practices are emerging that prioritize the development of improved vulnerability management processes. They focus on reducing risk across hybrid infrastructures, increasing efficiencies and scale across IT and security teams, freeing up talent to support strategic initiatives, and creating value-rich security programs.

63% of security leaders cited 10 or fewer vendors in their environment.

3 CISO Benchmark Study, Cisco, 2019

SCAN AND PATCH IS NOT GOOD ENOUGH

Many vulnerability management programs currently focus on patching as many critical-severity vulnerabilities as possible, as defined by the Common Vulnerability Scoring System (CVSS). This traditional approach relies on active scans to discover vulnerabilities, looks at generic severity scores, potentially includes some exploitability information and then works on deploying the patch (if one is available). While vulnerability assessment and remediation are fundamental pieces of a security program, the "scan and patch" approach leaves out crucial elements of the vulnerability management workflow, especially in how remediation priorities are set. Scanners usually don't take into account the network security devices that can shield against potential exploits. Without this vital understanding of network context, scanners may direct remediation resources to protected assets while ignoring ones that are exposed. Additionally, they can't recommend remediation outside of patches, which may not be available or not be the best option. This means that, in practice, they do little to reduce risk over time or enable rapid response to imminent threats.

Vulnerabilities which have the most pressing need for remediation could be hiding in plain sight

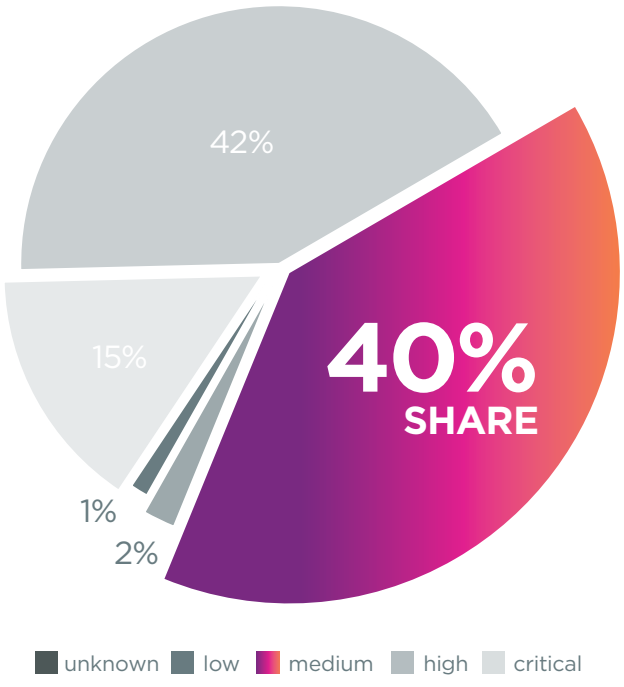
---

While CVSS scores are an important aspect of understanding the risk a vulnerability poses to an organization, it is also critical to know the likelihood of its exploitability. Some of the vulnerabilities which have the most pressing need for remediation could be hiding in plain sight: for example, a CVSS medium-severity vulnerability may be under active exploit in the wild while a critical-severity vulnerability has no exploit developed. In this case, the medium-severity vulnerability would pose a greater risk and is a higher remediation priority — even more so if it's exposed and unprotected by security controls.

MEDIUM-SEVERITY DOESN'T EQUATE TO MEDIUM RISK

The sophistication of hacking techniques is growing by the day, as is threat actors' confidence that they will be successful in their attempt to gain ransom. They are fully aware how important it is for businesses to maintain business continuity during the current crisis. If security programs do not evolve their remediation practices to identify how exposed each vulnerability is — regardless of its severity score — then they will be playing into their enemy's hand.

Consider this: there are likely going to be more than 20,000 new flaws to manage by the end of the year and 3,877 new medium-severity vulnerabilities were published over the first half of the year[4]. Due to current 'scan and patch' practices, many of these vulnerabilities are likely to sit unpatched and improperly managed by many organizations for a significant amount of time.



New vulnerabilities' CVSS scores by severity level in 2020

Medium-severity vulnerability count year-over-year

Traditional remediation practices immediately focus action on the 15% of critical-severity vulnerabilities, followed by the 41% of high-severity vulnerabilities. Which means that medium-severity vulnerabilities, which make up 40% of the share and have increased in count by 36% year on year, sit unpatched for a prolonged period of time.

Medium-severity doesn't equate to medium risk: hackers see these vulnerabilities as an opportunity. They know that security teams are distracted by remediating masses of critical – and high-severity vulnerabilities and know that they are ripe for attack.

This doesn't mean that they are going to use medium-severity vulnerabilities to immediately launch a devastating attack. They see these vulnerabilities as an opportunity to gain lateral movement within the security environment. Attack methods are increasing in sophistication — working with the knowledge that medium-severity vulnerabilities are going to be left untouched, threat actors are able to take advantage by first deploying a trojan, for example, before moving on to more disruptive malware like ransomware.

*Medium-severity vulnerabilities, which make up **40% of the share** and have **increased in count by 36%** year on year, sit unpatched for a prolonged period of time.*

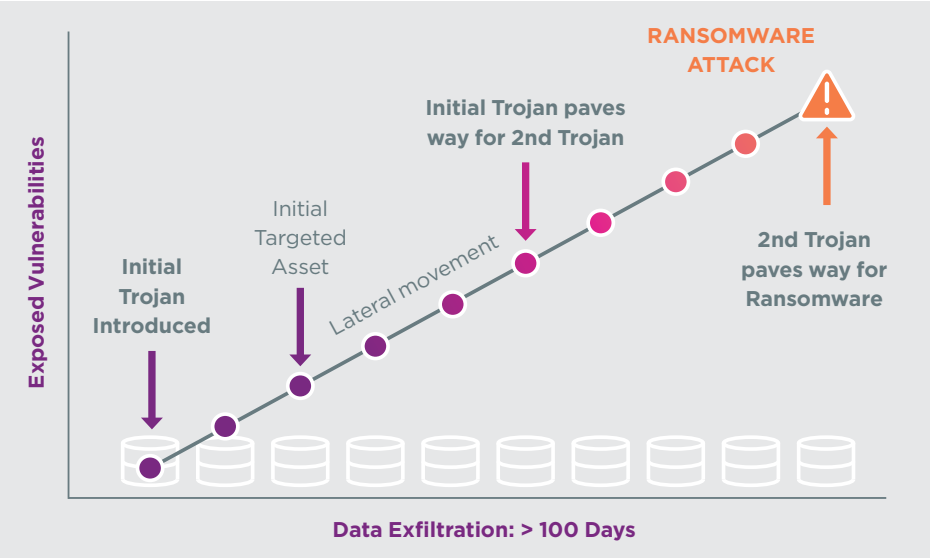
ATTACK CHAINS CAUSE DEVASTATING DAMAGE

Vulnerabilities can be chained together by an attacker to great effect. Contemplate this scenario: one vulnerability (say, with a medium-severity CVSS score) may allow an attacker to gain a foothold on a system under an account with very low privileges, while another vulnerability may allow an attacker to escalate privileges to an administrator level. In isolation, the medium-severity vulnerability can seem to pose very little risk. Thus, deprioritizing its patch would make sense from a resourcing perspective. But if an exposed medium-severity vulnerability is left open, it could provide a launch point for a threat actor to gain remote access with administrator level privileges.

In this example, it is clearly important for the security teams to have context-informed visibility so that they can understand the connection between vulnerabilities and how exposed they are to threats. They need insight that enables them to stop these attacks before they happen — they need to understand exposure so that they can effectively prioritize the patching of vulnerabilities.

72% increase in new ransomware samples

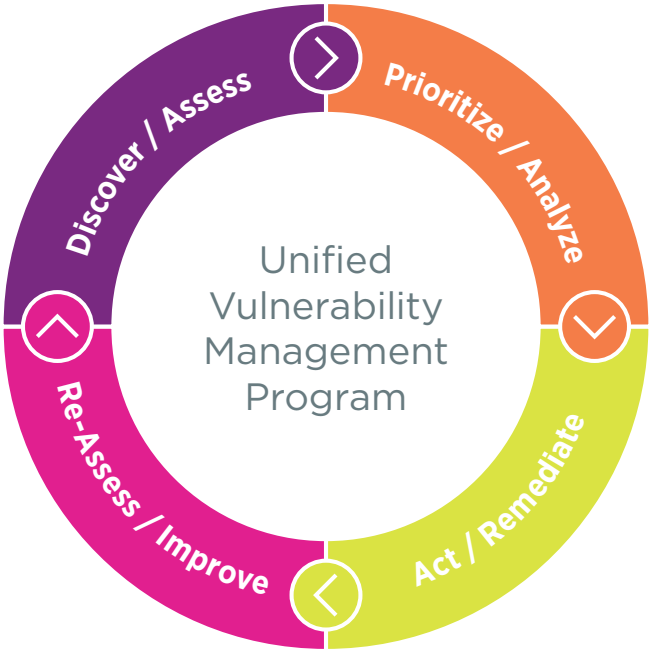
Hackers' increasing draw towards chained attacks is clear when you look at the increase in creation of new malware samples over the course of the year. Notable is the increase of new ransomware samples and trojans. Over the first half of 2020, the creation of new ransomware samples increased by 72% with trojans following a similar growth pattern. There are numerous examples of hackers using trojans in collusion with ransomware to carry out chained attacks. Consider the relationship between Emotet, Trickbot and Ryuk as one example; after the Emotet trojan is able to deliver another trojan, TrickBot, attackers are then able to move laterally throughout the network to deploy Ryuk ransomware.



Increasing sophistication of the attack chain is exploiting vulnerabilities: example ransomware attack

A ROADMAP TOWARDS IMPROVING VULNERABILITY MANAGEMENT PRACTICES

In order to address the rising volume of vulnerabilities along with increasingly sophisticated hackers, it is clear that security and risk management teams need to have full context and understanding of their attack surface with the characterization and prioritization of assets across the network, so that they can efficiently identify and remediate risk exposures that pose the greatest threat to the organization. The only way to achieve this is to move beyond simply scanning and patching towards taking a full life-cycle unified vulnerability management approach.



This is a pivotal time for security leaders who now have the opportunity to forge a more resilient security program than they had prior to the pandemic. The emergence of distributed workforces has accelerated the need for transformation, placing the CISO in a position of increased influence within the C-Suite and the board. The central role that they play in ensuring the success of any new transformation project has affirmed the importance of security as a business driver. But in order for the CISO to successfully transform the security function so that it can better enable business-critical initiatives, they first need to tackle the fundamental issues that are standing in the way of progress.

The existing problems with traditional vulnerability management and remediation practices, if left unaddressed, could lead to an increasing number of breaches. This should be a particular concern for CISOs at large enterprises. It is estimated that cybersecurity losses, globally, have totaled $1.82 billion between September 2019 to September 2020, an increase of 50% from the previous year, with larger organizations the most common targets[5].

With the impetus for change being clear, security leaders now need to build a roadmap to modernize their approach to vulnerability threat management.

Estimated cybersecurity losses
September 2019 to September 2020

$1.82 BILLION

50% increase

FIVE STEPS TO BUILD A MORE RESILIENT CYBERSECURITY PROGRAM

1

EVOLVE THE TECH STACK

To maximize investments, security leaders need to evolve their technology stack to deliver critical business outcomes and long term value. When CISOs are dealing with a bloated stack that delivers restricted value, too much time can be devoted to trying to fortify their legacy infrastructure when their focus could be better placed elsewhere. Rather than buying point solutions that tackle hyper-specific security issues, the CISO needs to build a technology stack that provides them with a holistic understanding of their organization's infrastructure. When looking at which technology to invest in, the CISO needs to prioritize solutions that enable them to integrate data, gain visibility of all vulnerabilities and assets within their expanded infrastructure, and deliver insights that will empower them to take decisive action.

2

GAIN FULL NETWORK VISIBILITY

Security and IT organizations need complete visibility and analytics to quickly map, validate and remediate vulnerabilities across all network, cloud environments and endpoints wherever they are. This is not an easy task. It requires the establishment of a mature and tightly connected security management framework that spans across their planning, implementation, and ongoing change management workflows.

3

IMPROVE DISCOVERY CAPABILITIES

Once visibility has been achieved, it is then important to build capabilities to discover all vulnerabilities within the security environment. A successful vulnerability management program starts with accurate vulnerability data. Active scanning is an important component of the discovery phase, but has its limits. Today's networks — encompassing cloud and operational technology (OT) — are filled with blind spots that scanners simply cannot cover. These blind spots need to be covered.

This can be achieved when disparate data repositories, such as patch and asset management systems, configuration data, threat intelligent feeds, and network security devices are brought together, with data normalized and modeled to infer the presence of vulnerabilities. If security leaders are able to achieve this, they will be able to passively detect vulnerabilities across their fragmented and dynamic security environment.

4

PRIORITIZE VULNERABILITIES BASED ON EXPOSURE

Moving towards a vulnerability management program that is led by an understanding of exposure starts by gleaning insight into the organization's current vulnerabilities, as determined during the discovery phase. This insight should then be enhanced with more information to better understand the implications of current vulnerabilities — this information needs to include conditions such as operating systems, versions, or other applications that would affect the exploitability of a vulnerability; exploitation effect on CIA values; NVD research on the vulnerability; a list of mitigation solutions; severity ratings from multiple sources, including CVSS scores; and a history of changes in the vulnerability as it relates to severity, exploitation, and available patches.

This should also be combined with external threat intelligence and internal network intelligence (including insight into network topology and security controls). All of this information should then be used to determine how exposed the vulnerability is within a network by simulating attacks on the network model created during the initial visibility phase.

5

FOCUS REMEDIATION WHERE IT'S NEEDED MOST

With effective discovery and prioritization practices in place, organizations are left with a smaller and more manageable number of vulnerabilities that they know require their immediate attention. Top priorities are vulnerabilities on important assets, exposed to a threat origin and with an active exploit. At this stage, the CISO and their team has a lighter workload and is better able to focus remediation where it's needed most.

BENEFITS OF EXPOSURE-BASED REMEDIATION

- Reduce complexity of vulnerability management
- Gain visibility and insight of your network
- Save time and resources through operational efficiencies via automation
- Focus action where it is most needed
- Respond faster and smarter to threats

To learn more visit https://www.skyboxsecurity.com/trends-report/

ABOUT SKYBOX SECURITY

Over 700 of the largest and most security-conscious enterprises in the world, rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. At Skybox, we don't just serve up data and information, we provide the intelligence and context to make informed decisions, taking the guesswork out of securely enabling your business at scale and speed. Our unified security posture management platform provides Security and IT teams complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization. And intelligently optimize security policies, actions and change process across all corporate networks and cloud environments. With Skybox, your security team can now focus on the most strategic business initiatives while ensuring your business remains protected.

We are Skybox. Secure more, limit less.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060