XM Cyber | See All Ways™

IBM

Cyber Exposure Management: You Can't Protect What You Don't Know

Yaşar Yüzer, IBM
Cyber Threat Management Services Leader
Germany, Austria & Switzerland

Michael A. Greenberg, XM Cyber
Director of Product Marketing

Table Of Contents:

Introduction

The world continues to grapple with a lasting pandemic, the shift from work-from-home to back-to-office, and geopolitical changes which have spawned a constant stream of mistrust. All of this equates to chaos, and in chaos, cybercriminals thrive. In this environment, companies experience an increase in breaches, and not surprisingly, related costs continue to soar.

Reaching an all-time high, the cost of a data breach[1] averaged USD 4.35 million in 2022. This figure represents a 2.6% increase from last year, when the average cost of a breach was USD 4.24 million. The average cost has climbed 12.7% from USD 3.86 million in 2020.

Most organizations invest in technology and processes to prevent cyberattacks – the average company deploys up to 50 tools[2] to protect their infrastructure. But cyber criminals are exploiting organizational silos, remote workers, the supply chain, and even national borders, to undermine the safety and security of critical systems.

Using various security solutions clearly helps to shed light on the many misconfigurations, vulnerabilities, and mismanaged credentials. But often, these solutions can not correlate the risks between those that attackers use to form attack paths across networks, compromising business-critical assets.

Research shows that on average, 75% of an organization's critical assets[3] can be compromised in their current security state. In 2021, phishing operations emerged as the top pathway to compromise organizations, using Ransomware as the number one attack method, followed by Server Access and Business Email Compromise[4].

In 2022, continuing the trend, there has been a rise in reported breaches involving multi-factor authentication bypass which steals tokens through phishing campaigns.

You Can’t Protect What You Don’t Know

As philosopher Sun Tzu wisely said, “To know your enemy, you must become your enemy.” Now is the time to not only understand your strengths and weaknesses, but to understand the tools and motivation of your adversaries.

So now let’s explore how organizations put themselves in the headspace of the attacker.

The first step is leveraging open source or subscription-based threat intelligence to provide meaningful visibility into each organization’s threat landscape, which clearly changes based on geography, industry, and organization-specific circumstances. It is equally important though to have a risk-based understanding of all the technical and procedural access points and attack paths that lead into the organization, both internally and externally, including those from third-party partners and vendors.

Taking it one step further is prioritizing the identified risks in relation to the organization’s defined critical assets. Being able to focus remediation efforts is a major contributor to being able to reduce cyber risk.

Once an initial understanding is achieved, the next step is to validate detection, prevention, and response capabilities. In simple terms, this means getting an understanding of the organization’s exposures and defining how to manage them.

Different Solutions and Methods on the Market

There are many different solutions and technologies that make the above steps scalable and sustainable, which we have bundled in six groups.

Attack Path Management

This group encompasses solutions that model and visualize how an attacker propagates the network by discovering critical attack paths and choke points.

Organizations are looking to get a universal, continuous view of their security posture, incorporating existing exposures and weaknesses that attackers leverage to compromise critical assets, along with security control gaps that fail to prevent attacks in the most cost-effective way to improve and meet compliance and enterprise security needs. With Attack Path Management, organizations can continuously reduce risk exposure by uncovering hidden attack paths to critical assets, identifying security controls gaps and prioritizing security exposures so they can focus remediation activities.

Attack Surface Management

These are solutions that provide continuous discovery, inventory, classification, and monitoring of an organization's external IT assets based on public data, intelligence, and active scans.

Attack surfaces have been rapidly expanding in recent years, thanks in part to digitization, cloud computing, and the increased popularity of remote work. This has given attackers a target-rich environment in which to operate.

Attackers have also started using complex tools to examine external attack surfaces, performing reconnaissance work, and gathering actionable information. This greatly increases the odds of a successful breach.

Breach and Attack Simulation

These are solutions that automate security posture assessments by continuously validating technical and procedural security controls between different segments of internal and external networks.

Most of the techniques used by adversaries are known and publicly documented. Testing security controls with known payloads is an effective way to understand the resilience of configuration and security architecture. As part of red or blue team activities, security operations teams gain visibility of capacity as well as detection and response capabilities.

Security Ratings

This collection of solutions rate external cyber posture by analyzing and simulating public data and threat intelligence.

But not all security ratings from various vendors are the same. Some may measure a single point in time, or an organization’s exposure in the moment. Others assign a rating based on ongoing program performance over time.

Security rating solutions provide organizations visibility in making better, smarter risk decisions for their own needs, as well as validating third parties which they work with.

Vulnerability Scanners

This group of solutions enable a regular process of identifying, assessing, reporting, managing, and remediating security vulnerabilities. It also helps see missing patches across internal and external endpoints and systems.

Vulnerability management is primarily used throughout the entire process of vulnerability discovery, prioritization, and remediation. Traditionally, solutions look for exploitable vulnerabilities using CVSS scoring, focused on the risk on the critical asset, and not the risk towards the critical asset. Vulnerability scanners are a proven solution to survey organizations' threat landscape and fulfill compliance requirements.

Penetration Testing & Red Teaming

These are exercises where a service provider acts as an adversary, attempting to identify and exploit potential weaknesses within the organization's overall cyber posture with Red Teaming, or specific applications using sophisticated attack techniques.

Penetration testing and red teaming enable internal security organizations to test their defensive capabilities during an actual attack.

With multiple options available, full visibility into cyber exposure may require more than one solution since technologies differ in scope, automation, coverage, and assurance.

For instance, **penetration testing** results will deliver highly confident results for a limited scope, but significant manual effort is required. And **vulnerability** scanning covers a wide range of assets in a nearly fully autonomous way, but the results need manual review due to a high percentage of false-positives.

Breach and attack simulations apply most known attack techniques between external and internal networks in a highly automated fashion, but due to their nature, are used on golden images to prevent operational risks. So for the applied path, the results will be close to reality, but coverage depends on the standardization maturity of each organization.

Attack surface management and security rating technologies provide a continuous overview of externally available assets and their security posture and any potential shadow IT. Unfortunately, this overview will not apply to the internal posture.

Attack path management creates an ongoing process for identifying exploitable attack paths to critical assets and help organizations identify their most critical exposures like misconfigurations, risky users, and software vulnerabilities across the hybrid environment. Since attack path simulations are carried out with telemetry data moved to the cloud, the analysis is not malicious, butas as such does not automatically trigger remediation and mitigation actions.

Using Solutions Effectively

When it comes to determining the right approach for your organization, it will also be dependent on the capacity to cope with the results provided. Investing in any technology or solution which cannot be properly managed obviously won't deliver the desired results.

None of the abovementioned solutions should be used in silos and without a defined governance model which, at the very least, defines the roles and responsibilities of different units managing the solution. Outputs of the solutions need to be aligned on well-defined key performance indicators.

As for all efforts in cybersecurity, automation should be used wherever possible. An output from one technology should trigger action for another one.

Some basic ideas may be:

Prioritize tickets for identified gaps in IT service management tools.

Prioritize patching requirements on servers or end points.

Optimize the efficiency and coverage of SIEM use cases.

Trigger SOAR playbooks based on relevant findings such as: quarantine servers or clients, block IPs, patch systems, disable users, etc.

Define new playbooks based on identified threat scenarios.

Align business goals and risk exposures through cyber risk dashboards that can easily be presented to decision makers.

Conclusion

Organizations need to understand the likelihood of compromise and the impact that could occur to business-critical assets to effectively close security gaps and reduce risk exposures. Most importantly, they need answers to the key questions:

Which threats pose the greatest risk to the organization?

How could an attacker take advantage of any security gaps or vulnerabilities?

Do we know our most critical exposures and how to mitigate them?

How effective are the security controls we use at preventing and detecting attacks?

Are we getting the best return from our security spend?

To better understand whether critical assets are safe, it's imperative to get visibility into how things change over time, and how those changes affect risk. Using the aforementioned solutions to enable predictive modeling of an attack is one way to do this. This approach provides a consistent predictive archetype that cuts through the noise of what can be bypassed and what cannot, and contextualizes this information within the framework of critical assets.

References:

1 IBM Cost of a Data Breach Report 2022
2 IBM Cyber Resilient Organization Study 2021
3 XM Cyber Impact Research Report 2022
4 IBM X-Force Threat Intelligence Index 2022

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty. IBM operates one of the broadest and deepest security research, development, and delivery organizations. Monitoring more than 4.7 trillion events per month in more than 130 countries, IBM holds over 10,000 security patents. To learn more, visit ibm.com/security. Join the conversation in the IBM Security Community.

ibm.com

IBM

About XM Cyber

XM Cyber, a Schwarz Group company, is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk. By continuously uncovering hidden attack paths to businesses' critical assets and security controls gaps across cloud and on-prem environments, it enables security teams to remediate exposures at key junctures and eradicate risk with a fraction of the effort. Many of the world's largest, most complex organizations choose XM Cyber to help eradicate risk. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel. XM Cyber was acquired by the fourth largest retailer in the world, Schwarz Group in November 2021.

xmcyber.com

XM Cyber