POINT OF VIEW

Securing the Future

Embracing Complexity in Cybersecurity for Hybrid Cloud Environments

We're all in this together. That's the new realization concerning cybersecurity. It's necessary because we face far different cyber threats than we did 15 years ago and what we have been doing to stop them isn't working. In 2022, more than 4,100 publicly disclosed data breaches occurred equating to approximately 22 billion records being exposed. How can that be with the proliferation of security tools that organizations have invested in over the past decade? It almost seems like two steps forward three steps back.

EVOLVING SOLUTIONS

We aren't talking about underfunded public sector organizations or small businesses that may lack internal security aptitude. Organizations impacted included highly recognizable FORTUNE 500 organizations. Some of these attacks weren't even the result of a direct compromise. For instance, attackers were able to gain access to data from Shell PLC and the U.S. Energy Department by exploiting a third-party file transfer utility used by some of its employees. That's all it takes, and that's why organizations – from IT to the executive suite - must all be in it together to stay safe.

THE NEED FOR ACTION

To be successful, a business must be able to operate in a safe environment. The next time you board a plane, stop to think about all the people that contribute towards the safety of your flight. It's not just the captain who is responsibility for flying the plane. Mechanics ensure that the mechanicals of the plane are working optimally before takeoff. Air traffic control operators watch over the flight's trajectory to ensure a clear flight path. Flight attendants ensure that all passengers follow safety regulations. Even the passengers themselves are involved as they are told upon entering the airport to be aware of their surroundings and suspicious behavior – and they can't forget to buckle their seat belt. It is this "togetherness" approach that makes air travel the safest mode of transportation available. In fact, according to a 2023 Harvard study, your odds of being in an accident

Use Case

SOLUTION:

SEIM/SOAR/MDR

CHALLENGES:

- Security analysts are overwhelmed with additional data streams from an ever-increasing amount of security monitoring solutions (e.g. EDR, NDR, IDR, CloudSec, etc.)
- Security team is experiencing alert fatigue and/or inadequate in-house staffing and expertise
- Organization is missing true indicators of compromise

HOW WE HELP:

- Implement unified data sources (SIEM) and improved detection capabilities (threat intelligence and AI) with automated event correlational and consolidation related detections (MDR and AI)
- Assist with defining processes and common response actions in order to automate (SOAR)

RESULT:

- Detections streamlined with improved triaging and automated responses

The chance of your company experiencing a data breach is one in four. That figure doesn't include DDoS attacks and purely destructive ransomware outbreaks.

Use Case

SOLUTION:

Tabletop

CHALLENGES:

- Concern about effectively responding to security incidents given the ever-evolving threat landscape, the increasing complexity of attacks, and constant shifting of enterprise footprint (mobile, cloud, etc.)

HOW WE HELP:

- Lead a collaborative incident response tabletop with key stakeholders, tailored to threats facing their organization

RESULT:

- Gaps identified in incident response processes while simultaneously engaging business leaders throughout the organization
- All stakeholders educated, ensuring mutual agreement on everyone's role during incident response and gained feedback from all parties to improve the response plan

during flight is one in 1.2 million and the chances of an accident leading to a fatality is one in 11 million. Your chance of a car accident fatality is one in 5,000. In that context, it's even more alarming that the chance of your company experiencing a data breach is one in four. That figure doesn't include DDoS attacks and purely destructive ransomware outbreaks. Clearly breaches happen regularly.

FOCUSING ON THE WRONG THINGS

Organizations today place a lot of emphasis on compliance, and for good reason. There are stiff penalties for GDPR or CCPA non-compliance. But compliance does not equal security. You can meet every compliance regulation and still not be secure. Oil companies, healthcare organizations and banks, in spite of being continually audited, are continually compromised. A confirmation of compliance is not a get out of jail card. It just means you have followed the applicable regulations.

The reason why organizations continue to be compromised by threat actors is not due to a lack of trying. Many organizations have assembled an abundance of security tools. One study showed that an overabundance of security tools was the number one challenge of threat detection and remediation. The average organization now deploys 45 security solutions and uses 19 different tools when responding to a cybersecurity incident. The reality is some tools never get implemented, many aren't optimized, and most work in a disjointed fashion that creates gaps. More tools mean more complexity, and complexity creates fertile ground for hackers.

MORE INFORMATION DOESN'T MAKE US SAFE

IT estates have rapidly expanded as companies have transitioned to hybrid and multi-cloud enterprises. As a result, cybersecurity teams have turned to SIEMs to collect and aggregate logs, metrics, and alerts from across the many devices spread across their vast planes of attack surfaces. The premise makes sense; the better informed you are, the more secure you are. Unfortunately, that assumption doesn't play out. According to a 2023 study, the average SIEM fails to detect an alarming 76% of the tactics and techniques used by active hacking organizations as outlined by the MITRE ATT&CK framework. The problem is not the SIEM itself. Its ineffectiveness stems from the fact that it needs to be configured correctly and maintained as threats evolve and the attack surface changes with new IT capabilities.

SECURITY AND MODERN OPERATIONS

In the era of digital transformation, Security must be strategically intertwined with Modern Operations. As business operations expand beyond traditional perimeters into cloud and hybrid environments, establishing a robust and adaptive security posture has become as critical as ensuring seamless operations. Strategically placed defense mechanisms safeguard a business's most valuable assets such as data, applications, platforms, and infrastructures against both internal and external threats while a well-designed strategy can ensure asset security, regulatory compliance, and seamless business operations.

Use Case

CLIENT:

vCISO/Assessments

CHALLENGES:

- Concern that existing cybersecurity investments are not being fully utilized or adequately protecting the organization against modern threats

HOW WE HELP:

- Assess the current technologies and capabilities
- Optimize configuration and improve integrations of existing technologies so they are more effective
- Recommend and/or augmented existing toolset with missing technologies, as needed, ensuring the new tools integrate with existing investments

RESULT:

- Organization has a newly designed roadmap with prioritized recommendations to improve the security posture

The elements of Security in Modern Operations don't just mitigate threats and foster regulatory compliance. It also becomes a catalyst for business continuity, consumer trust, and growth. By emphasizing security at the forefront of their IT operations, organizations are better equipped to steer through the shifting threat environment, securing both their operational integrity and reputation.

SECURITY AS AN ENABLER

One of the inherent problems for cybersecurity since the beginning is that it is often viewed as an obstacle to getting things done, even as an annoyance. At Evolving Solutions, we believe that security should be a business enabler. Organizations can skillfully calibrate their security investments to both mitigate business risk and foster the pursuit of fresh business opportunities. Your security investments should garner a ROI like any other investment in your business and that return comes in the form of creating a safe environment that your business can prosper in. However, depending exclusively on conventional strategies like focusing on tools, accumulating information, and maintaining compliance will have you fall short of the mark.

FROM SECURITY TO SAFETY

The evolving threat landscape and sophisticated attack techniques mean that no organization is immune to a breach. The sources of potential threats extend beyond external bad actors (ransomware, malware, unauthorized access, etc.). Internal risks, whether driven by employee negligence or malicious intent, prove equally serious. Acknowledging that breaches are the new reality and proactively working towards their prevention can significantly reduce their impact.

Evolving Solutions can help you bring together people, processes, and technology to effectively combat threats and move your organization from secure to safe. Our team of security experts will sit down with you to understand your objectives, undertake tabletop exercises to identify gaps and lessons learned, and create a roadmap for you to deal with the threat landscape.

The Evolving Solutions team incorporates its recommended security measures directly within its own operations. We believe our efforts and the efforts of our clients are best served by transitioning from exclusively a prevention mindset to an approach that emphasizes resilience, data integrity, and system stability to ensure a safe environment for business operations.

Tabletop Exercise

Evolving Solutions Cybersecurity Tabletop session is a collaborative simulation-based exercise that brings together key stakeholders and participants to discuss and practice their response to various cybersecurity incidents in a controlled environment. Our team moderates the discussion and walks participants through real-world scenarios and challenges related to cybersecurity breaches, attacks, or threats.

Why? Tabletop exercises are an essential component of an organization's cybersecurity preparedness and can significantly enhance the ability to respond effectively to real-world cyber threats. They allow organizations to evaluate their preparedness, identify weaknesses, improve coordination, and build a more resilient cybersecurity defense. These sessions are a core part of our approach to move an organization from secure to safe.

Many organizations conduct tabletop exercises as part of check-the-box compliance requirements, but they are not realizing the benefits. This is where Evolving Solutions can help. We combine years of incident response experience with a deep understanding of technical and business challenges to provide a tailored experience which results in clearly identified gaps and actionable objectives. This approach actively engages stakeholders throughout the organization, incorporating multiple perspectives, and ultimately achieving consensus on the importance of cyber resiliency and an improved understanding of everyone's role.

Our holistic approach focused on the following three areas:

1. **Tabletop Exercise:** This collaborative exercise is designed to testing and understanding existing capabilities of the organization in a real-world scenario incorporating the unique risks that face the organization. It involves the assessment of an organizational capabilities and maturity level across various parts of the organization, identifying gaps, and recommending targeted improvements to bolster an organization's cyber resilience.

2. **Cyber Defense Matrix:** Mapping different control frameworks and analyzing security weaknesses to create actionable roadmaps tailored to the organization's requirements. By using a matrix to plot various cybersecurity technologies, processes, and team capabilities, organizations can ensure they have a balanced and comprehensive cybersecurity defense strategy that covers all critical areas of cybersecurity. This process helps identify any potential gaps in defenses and allows organizations to allocate resources effectively to improve their overall cyber resilience.

3. **Balancing People, Process, and Technology:** Cybersecurity requires a balance between people, processes, and technology. If even one of these is out of balance, the result is generally unsuccessful outcomes. For example, having the right technology without supporting people and processes leads to shelfware. Whereas having the right people and processes without supporting technology, you have a burden to scale. Cyber resilience – success – is achieved when all three are balanced and operating efficiently.

This approach ensures security is integrated into the organization's operations rather than being viewed as a standalone roadblock or check-the-box compliance.

2023 Top 5 Cybersecurity Threats

1. **Phishing and Social Engineering:** Phishing attacks involve deceptive emails, messages, or websites designed to trick individuals into revealing sensitive information, such as passwords or credit card details. These deceptive tactics have emerged as major cyber threats, exploiting human psychology and technological vulnerabilities to gain unauthorized access to sensitive information or manipulate victims for malicious purposes. Phishing and Social Engineering attacks are often a precursor to other attacks such as ransom attacks, business email compromise, and even insider threats.

2. **Business Email Compromise (BEC) / Corporate Account Take Over (CATO):** These attacks usually target specific roles or employees within your organization. Threat actor motivation is usually focused on financial gain such as gaining unauthorized access to financial accounts to control and manipulate transactions (such as wire or gift-card fraud), stealing sensitive or secret information, or leveraging the compromised employee's authority to convince others to take specific actions – potentially leading to another person in your organization or even outside of your organization to become an unsuspecting accomplice or victim. In a cloud-connected world, threat actors can compromise your data without ever being in your network.

3. **Ransom Attacks:** Ransom attacks have become increasingly sophisticated, causing substantial financial losses, disruptions to critical services, and compromising sensitive data. The consequences can be devastating, ranging from the loss of intellectual property and financial resources to reputational damage and potential legal repercussions. Many attacks leverage ransomware which is a specific type of malware that encrypts files and demands a ransom for their release. Many ransom attacks no longer use ransomware. Threat actors are now weaponizing commercially available tools with malicious intent – largely to conduct data exfiltration and ransom guarantees not to release the stolen data.

4. **Vulnerabilities:** Vulnerabilities in cloud infrastructure, applications/ software, endpoints, and networks have all played a significant role in recent attacks. Zero-day vulnerabilities, those which are known to have imminent risk of exploitation at time of announcement, are leading the risk and challenging status quo patch management philosophies and programs. Speed of response is essential as well as managing and reducing attack surfaces. Vulnerability risks highlight the impact of misconfigurations (blocking-and-tackling), insecure APIs and automation, and immature programs.

5. **Insider Threats:** 19% of security risks also originate from within an organization. This can be malicious insiders with authorized access compromise systems or accidental insiders who, due to human error, create problems (phishing, exposing data, etc.). Detecting and preventing insider threats requires a multi-layered approach that includes background checks, access controls, monitoring systems, training, and ensuring a culture of security awareness within an organization.

SECURITY IS A JOURNEY

Security is not a destination; it is a journey. There is no arrival point at which you are totally safe because new exploits, tactics, and attack techniques are constantly in flux. That is why we recommend staying engaged and routinely assessing and updating your security roadmap to keep pace with emerging threats that will inevitably arise. We don't subscribe to the belief that tools alone will prove sufficient to secure your organization throughout this journey. Our balanced approach is:

- **Comprehensive:** Evolving Solutions understands that IT systems and operations are the backbone of a modern organization. Any disruption can have significant financial and operational impact. This viewpoint is based on an understanding of and alignment to the goals and objectives of the entire organization. Our team understands the necessity to look at the entirety of an organization's technology stack and the importance of reevaluating and adjusting strategies every 12-18 months to counter ever evolving risks and exploitive tactics. This allows us to navigate the entire cybersecurity landscape and bridge disciplines and teams across the organization to deliver better outcomes.

- **Holistic:** Our approach extends beyond compliance to regulatory standards. We have a proactive, holistic approach to protecting information systems and data, that includes technology, processes, people, and risk management, rather than simply focusing on meeting minimum regulatory requirements.

- **Effective:** We know that breaches happen. Our job is to help you:
  - Effectively identify and manage cyber risks
  - Minimize disruption, system downtime, and data loss
  - Safeguard data from unauthorized access, use, or disclosure
  - Adhere to laws, industry standards, and organizational policies governing the collection, storage, and usage of sensitive information
  - Avoid potential financial losses, penalties, reputational damage, and the costs associated with incident response, recovery, and remediation

Our approach helps organizations establish a strong and resilient security posture to protect the organization. We do this by providing quick start projects for rapid results, health checks, and ongoing checkpoints to ensure success.

EVOLVING SOLUTIONS SECURITY PRACTICE

Evolving Solutions works seamlessly across organizations. By bridging disciplines and teams, we ensure the delivery of actionable insights and security solutions that comprehensively address an organization's entire business landscape. We actively focus on shifting organizations from a reactive "secure" approach to a proactive "safety" approach, providing the foundation needed for business enablement. In the same way we have helped companies transform IT operations environments, we can help you take a different approach to ensuring a safe and resilient environment for reliable business operations. Let us show you how.

EVOLVING SOLUTIONS

Moving Your Organization from Secure to Safe.

Let’s get to work.

 ESI-091423-A101