CYBERSAFE SOLUTIONS | BEST PRACTICES WHITE PAPER

Cybersafe Solutions Best Practices

To analyze our client's risk posture and challenges, the Cybersafe Solutions Security Operations team leverages the following approach and security methodology. This fundamentally unique approach to cyber risk management allows Cybersafe to advise on a comprehensive cybersecurity program that incorporates preventative and detection measures.

The following security controls increase the organization's ability to prevent, detect and respond to a cybersecurity event. By implementing each control, an organization can minimize the impact of a cyber event, attack, or breach should it occur, and help respond in a responsible and cost-effective manner.

The following considerations were made when compiling this documentation:

- **Cyber Insurance:** Ineffective cybersecurity hygiene has a major impact on cyber insurance rates. While customer demand has been surging for cyber insurance, cyber insurers' payouts are also increasing.
- **Recent Trends on Disclosures of Regulated Data Loss:** Trends show increased scrutiny from regulatory and compliance standards.
- **Disclosures of Sensitive Unregulated Information:** Exposure of sensitive information, intellectual property, company data or system passwords, employee salaries, internal communications, strategic plans, and other data that should not be made public.
- **System or Operational Downtime:** Taking a reactive approach to cyber events can cause system downtime and prolong recovery, investigation, and remediation. According to recent trends, this can also cause a significant loss of employee productivity.
- **Increased Risk of Lawsuits or Fines:** It is possible that the organization could be subject to a lawsuit or other sanction due to higher visibility, increased pressure from sensitive information, or adverse effects on a certain party.

The following is intended to serve as a guideline for a comprehensive framework of security practices and benefits of an information security program. The content of this document should be viewed as an adequate starting point for internal discussions within the organization and key points to consider when discussing appropriate measures and how it pertains to general risk acceptance.

SECURITY AWARENESS TRAINING

Building a security awareness and training program is a critical element in any security posture. Failure to give attention to the area of security awareness training puts an organization at great risk, as cybersecurity is ultimately as much a human issue as it is a technology issue. The first step of implementation is confirming that all users are aware they have a role to play in the success of a security awareness and training program.

A cybersecurity program is also not complete without training end-users on security policy, procedures, and techniques. As your front line of defense, it is crucial for end-users to understand their part in protecting your organization as well as remaining vigilant with frequent testing through simulated phishing. An effective program would include insight into the various management, operational, and technical controls necessary and available to secure your internal infrastructure. An informed user can develop the necessary skills to carry out their assigned duties effectively—for instance, in reporting suspicious behavior to the appropriate individuals.

CYBERSAFE SOLUTIONS®

COMPLEX PASSWORD & PASSWORD MANAGEMENT

As humans, we have a limited capacity to memorize complex passwords and as a result, users often choose passwords that can be easily guessed. To address resulting security concerns, many have adopted rules and introduced policies to increase the complexity of each. For example, an organization may require the user to choose passwords constructed using a mix of character types, such as at least one digit, an uppercase letter, and a symbol. Breach analysis trends currently show that the benefit of such rules is not nearly as significant or impactful as initially thought.

Trends also demonstrate that many attacks associated with password use are not affected by complexity and length, but rather, by threat actors leveraging behaviors such as keystroke logging, phishing, and social engineering attacks.

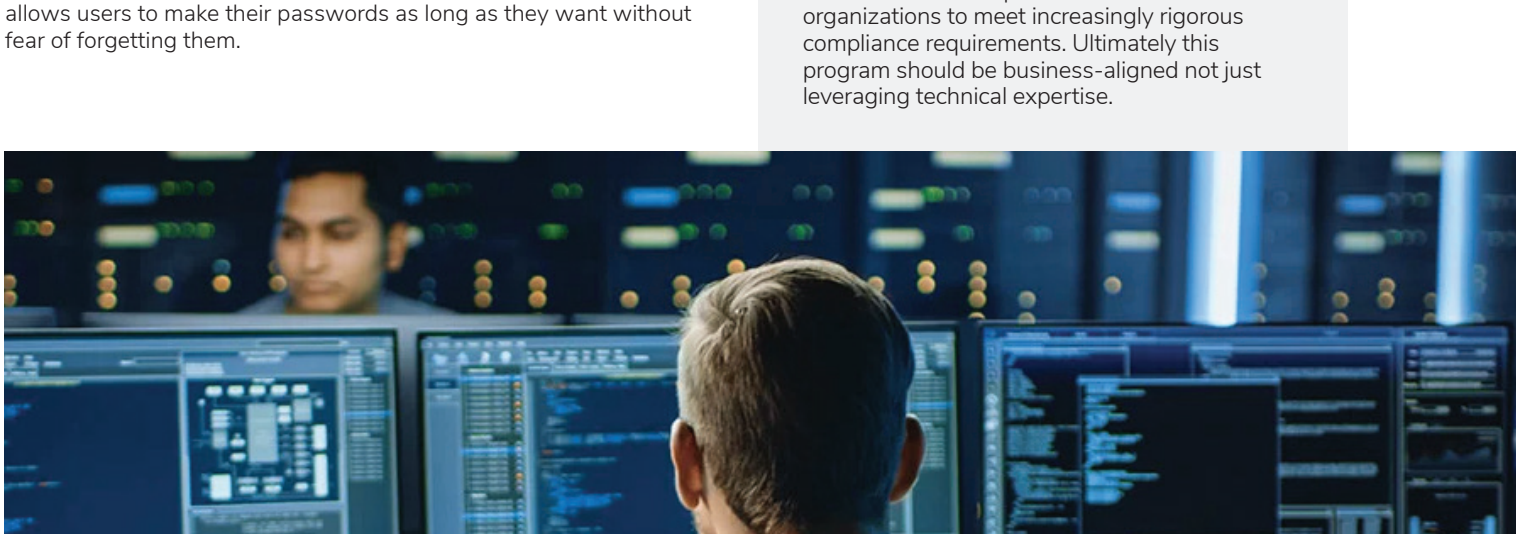
Alternatively, a frequently addressed issue is the element of password reuse. Users' password choices have now become very predictable, so attackers are likely to guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as "Password1!" or "Summer 2022." For this reason, it is recommended that passwords chosen by users be compared against a blacklist of unacceptable passwords. This list should include passwords from previous breach data, dictionary words, and specific words, and organizations should adopt robust policies that take these concerns into consideration. Implementing a password management system also allows users to make their passwords as long as they want without fear of forgetting them.

IDENTITY & ACCESS MANAGEMENT

Like our previous topics, traditional security programs often had a similar point of failure: the user and their password. Identity and access management (IAM) can narrow the points of failure and introduce another line of defense by confirming that the user, software, or hardware through authenticating their credentials against a database.

Identity and access management is a fundamental and critical cybersecurity capability. By design, IAM is the discipline that enables the right individuals to access the right resources at the right times. For example, an organization can implement the principle of least privilege and grant only the appropriate level of access to specific user groups. Instead of a username and password allowing access to an entire software suite, IAM allows for a far narrower scope.

IAM addresses the mission-critical need to ensure appropriate access across increasingly complex and distributed technology environments. This practice also allows organizations to meet increasingly rigorous compliance requirements. Ultimately this program should be business-aligned not just leveraging technical expertise.



CYBERSAFE SOLUTIONS®

SECURITY UPDATES & PATCH MANAGEMENT

Enterprise patch management is the process of identifying, prioritizing, acquiring, installing, and

verifying the installation of patches, updates, and upgrades throughout an organization. Adequate patch management is now more important than ever because of businesses' increasing reliance on technology.

Threat actors often look for systems that are not being properly maintained as their first step in exploitation.

- **Software maintenance** includes patching—applying a change to installed software—such as firmware, applications, or operating systems, to correct functionality or security problems and add new capabilities.
- **Enterprise patch management** involves identifying, prioritizing, acquiring, installing, and verifying installation of patches, upgrades, and updates throughout an organization.

In past perimeter-based security architectures, most software was operated on internal networks protected by layers of network security controls. While patching was generally ranked on the list of priorities to reduce the likelihood of compromise, it was not always considered mission-critical.

With recent trends, patching has become one of the most critical elements in protecting an organization. Recommendations are also made to take a Zero Trust approach to security (see below). Within modern infrastructure, the concept of the perimeter largely does not exist. Many technologies are currently directly exposed to the internet as a normal business practice.

From a cybersecurity standpoint, this introduces a significantly greater risk of compromise. Relevant computing technologies include information technology (IT), operational technology (OT), Internet of Things (IoT), mobile, cloud, virtual machine, container, or other types of assets. Patching is vital for reducing risk to those individual assets.

ENDPOINT SECURITY & EDR

In endpoint security & endpoint detection and response (EDR), safeguards implemented through software protect end-user machines such as workstations and laptops against attack (i.e., antivirus, personal firewalls, host-based intrusion detection and prevention systems, etc.).

As attackers double down on their offensive approach, they have become well organized and well-funded, ultimately allowing them to develop new skill sets. Adversarial groups are currently being tracked as they deploy new tactics and techniques with the intention of obfuscating defenses, oftentimes by leveraging built-in windows tools to further exfiltrate their attack.

Traditional and legacy anti-virus has historically been trailed in detecting these types of behaviors. Organizations are advised to invest in a next-generation technology that goes beyond the traditional signature-based prevention. Best practice today allows security teams to prevent, detect, and respond to modern attacks regardless of delivery vectors.

Aside from being signature-based, what primarily distinguishes EDR from endpoint protection platform (EPP) and legacy antivirus (AV) solutions is that these earlier security solutions were based on prevention alone—an inferior model. In contrast, EDR provides the enterprise with visibility into what is occurring on the network. Considerations should be made from a NIST perspective: identify, protect, detect, respond, and recover.

CYBERSAFE SOLUTIONS®

DNS & WEB FILTERING

DNS filtering is the process of using the Domain Name System to block malicious websites and filter out harmful or inappropriate content. Through this process, an organization can confirm its data remains secure and allows for control over what its users can access on company-managed networks. You may be accustomed to discussing this process as part of a larger access control strategy.

Configured DNS resolvers should also act as filters by refusing to resolve queries for certain domains that are tracked or listed within a blacklist—resulting in users being unable to access those domains. Alternatively, organizations can leverage an allow list to ensure access to specific domains.

For example, say an organization were to receive a phishing email resulting in the user or group of users clicking a malicious link. If that malicious site is within the organization's blacklist, the DNS resolver will block the request, prevent the connection, and ultimately thwart the phishing attack.

A secure web gateway (SWG) can protect company data and enforce security policies. It should exist between the users and the internet, functioning as a filter to stop unsafe content from web traffic from making its way into an organization.

Secure web gateway products contain these technologies:

- URL Filtering
- Anti-Malware Detection & Blocking
- Application Control

SWGs may also include data loss prevention (DLP), content filtering, and other internet traffic filters.

ZERO TRUST

It was previously noted that the concept of the perimeter has become a legacy school of thought in many organizations. Within modernization, a typical enterprise's infrastructure has grown increasingly complex. A single organization may operate several internal networks, remote offices with their own local infrastructure, remote and/or mobile individuals, and cloud services.

In many organizations, their information security practices did not scale to provide visibility into these new threat vectors. In some cases, these moves have inadvertently circumvented existing on-premise security solutions. For many, there is no single, easily identified perimeter for organizations allowing attackers to move laterally across their organization while going undetected.

A zero trust architecture is based on zero trust principles, and is constructed to prevent unauthorized access and limit internal lateral movement. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (local area networks versus the internet) or based on asset ownership [corporate owned or bring-your own device (BYOD)].

Authentication and authorization—both subject and device—are discrete functions performed before a session to an organization's resource is established. Zero trust is a response to enterprise network trends that include remote users, BYOD, and cloud-based assets that are not located within an enterprise owned network boundary. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the system accessing it.

CYBERSAFE SOLUTIONS®

EMAIL & PHISHING PROTECTION

As the world shifted to virtual and remote work, email is more of a core component of the modern distributed workforce than ever before. This has resulted in it being one of the most exploited threat vectors.

An adequate information security program should include techniques for authenticating a sending domain, ensuring email transmission security, and ensuring email content security.

Security best practices for email begin by leveraging records and keys stored in the Domain Name System (DNS) by one party and extracted from there by the other party. With modern increased reliance on the DNS, there was the development and widespread adoption of the DNS Security Extensions (DNSSEC) to provide source authentication and integrity protection of DNS data.

Best practice within email includes authenticating the sending domain to protect senders from spoofing another's domain and initiating messages with illegitimate content. It also protects against malicious actors modifying message contents in transit.

Here are some email best practices:

- Sender policy framework (SPF) is the standardized way for a sending domain to identify and assert the authorized mail senders for a given domain.
- Domain keys identified mail (DKIM) is the mechanism for asserting sending servers and significantly reducing man-in-the-middle content modification by using digital signatures generated from the sending mail server.
- Domain-based message authentication, reporting, and conformance (DMARC) allows email senders to specify policy on how their mail should be handled, the types of security reports that receivers can send back, and the frequency of reports.

Standardized handling of SPF and DKIM addresses the unknown component about whether a given message is authentic. This practice should be used to benefit organizations and their security team by allowing a better understanding of quarantining and rejecting unauthorized mail.

***Information Technology and Security Teams can compare the "from" address in the message to the SPF and DKIM results, if present, and the DMARC policy in the DNS. The results are used to determine how the mail should be handled.*

**Man-in-the-middle attacks can intercept cleartext email messages as they are transmitted between mail relays. Any bad actor that can passively monitor network traffic can read such mail as it travels from submission to delivery systems. Email message confidentiality can be assured by encrypting traffic along the path*

CLOUD SAAS BACKUP

Remote backup services can help protect your data in the event of natural disasters, hardware failure, or local device infection due to malware or ransomware.

Cloud services have increased in popularity over the years as they introduce an element of convenience that many organizations did not have beforehand. These platforms give users on-demand access to data and applications anywhere you have an internet connection. In many cases, this helps eliminate the need for organizations to invest in networks, servers, and other on-premises hardware.

In some cases, cloud SaaS backups have provided less technical users with a false sense of security. Understanding the risk posture associated with cloud platforms begins with better understanding the platform itself. Many cloud service providers can require additional security controls such as multi-factor authentication (MFA) upon log in and encrypting user data within the platform. These security controls are critical in protecting these assets. However, cloud users have little or no direct control over their data or knowledge of their cloud service provider's security practices.

Due diligence during vendor evaluation is extremely important when picking a service provider. Consider asking questions suc as:

- "Is this a shared cloud?"
- "What type of security measures protect the hardware that stores, processes, and transmits company data?"
- "How do you prevent your data from leaking to other customers on its cloud?"

CYBERSAFE SOLUTIONS®

DATA ENCRYPTION

Encryption is often described as a security control that is frequently used to provide confidentiality protection for data. This concept is simply a mathematical transformation used to scramble data requiring protection (plaintext) into a form not easily understood by unauthorized people or machines (ciphertext). The plaintext, after being transformed into ciphertext, appears random and does not reveal anything about the content of the original data. The security benefit of implementing proper encryption practices is that once the data is encrypted, it is not able to be understood by any person or machine.

Within the modern landscape, encryption is widely used in many computer applications to protect data in transit and at rest. In some applications of secure web browsing, using secure socket layer (SSL) or transport layer security (TLS) protocols, the role of encryption may be transparent to the user. In other implementations, the user may be required to enter a password to encrypt or decrypt the protected data.

Another form of encryption is achieved by using secure/multipurpose internet mail extensions (S/MIME) which allows for emails to be encrypted by the sender and then decrypted by the intended recipient. The benefit of implementing this security control is that these email messages can only be read by the sender and the intended recipient(s).

Internet protocol security (IPsec) network layer security protocols are another form of encryption that are commonly used to establish virtual private networks (VPNs) between two ends of communication in an organization network. This allows for encrypted messages to be exchanged between them.

The SSL protocol and its successor—transport layer security (TLS)—are the primary end-to-end security protocols used to protect the information in transit. The most common usage scenario for these protocols is a web browser. Using SSL and TLS can allow for encrypted messages to be sent between a web browser and a web server which cannot be accessed or decrypted by an unauthorized party.

Taking a comprehensive approach, you can utilize encryption to protect data at rest such as data stored on hard drives, USB drives, and other end-user storage devices. For instance, in the event an encrypted hard drive is in possession of an unauthorized user, the encrypted data in the hard drive is useless because the user cannot reproduce the plaintext from the hard drive without the assigned key.

UNIVERSAL ENDPOINT MANAGEMENT

Unified endpoint management (UEM) as a tool or platform that provides an agent or agentless management of endpoints—such as workstations and mobile devices—through a single console.

UEM provides a user-centric view of devices across device platforms. It allows information technology (IT) teams to have access to an aggregate of telemetry and signals from identities, apps, connectivity, and devices to inform policy and related actions.

UEM facilitates numerous benefits for businesses:

- Aggregate and analyze technology performance and employee experience data.
- Integrate with identity, security and remote-access tools to support zero trust access and contextual authentication, vulnerability, policy, configuration, and data management.
- Manage nontraditional devices, including internet of things (IoT) devices.

Many UEM solutions provide visibility in the following areas:

- Authorized/Unauthorized Device Inventory
- Authorized/Unauthorized Software Inventory
- Secure Endpoint Configurations
- Administrative Privileges Control

Adopting a UEM solution can reduce organizational fragmentation and increase visibility into suspicious or abnormal activity across an organization's endpoints. Ideally, this practice will better inform decisions of analysis and prioritization of corrective action.

NETWORK SECURITY (ADVANCED THREAT PROTECTION)

Network infrastructure devices are the components on a network that transport communications needed for data, applications, services, and media. These devices often include routers, firewalls, switches, servers, load-balancers, intrusion detection systems, domain name systems, and storage area networks.

These devices are often ideal targets for threat actors because most or all organizational and customer traffic must pass through them. **For instance:**

- An attacker with a foothold on an organization's gateway router can monitor, modify, and deny traffic to and from the organization.
- An attacker with a foothold on an organization's internal routing and switching infrastructure can monitor, modify, and deny traffic to and from key hosts inside the network and leverage trust relationships to conduct lateral movement to other hosts.
- Organizations that use legacy, outdated, or unencrypted protocols to manage hosts and services are among the most vulnerable to credential harvesting, as whoever controls the routing infrastructure of a network controls the data flowing through the network.

Implementing a security control of segmentation is an excellent way to reduce risk. Proper network segmentation is an effective security mechanism to prevent a threat actor from the lateral movement if they successfully access an internal network.

The concept of segregation is accomplished when an information security team separates various parts of the network based on role and functionality.

Traditional network devices such as routers can also be separate local area network (LAN) segments. It is best practice to place routers between networks to create boundaries, increase the number of broadcast domains, and effectively filter users' broadcast traffic. These boundaries can contain security events or threat actors by restricting traffic to separate segments. Modern practices can even shut down segments of the network during an intrusion—restricting adversary access.

It is recommended all organizations implement and follow the principles of least privilege and need-to-know when designing network segments. If an individual or user group does not need access to something, do not provide it to them. To streamline this process, an organization should confirm it is separating sensitive information into network segments.

Another best practice is to utilize virtual local area networks (VLANs) to isolate a user from the rest of the broadcast domains. Using virtual routing and forwarding (VRF) technology can allow an organization to segment network traffic over multiple routing tables simultaneously on a single router. Additionally, implementing a virtual private networks (VPNs) will allow for a secure connection by tunneling through public or private networks.

When evaluating network security practices, an organization should also evaluate risks associated with user-to-user communication, such as workstation-to-workstation. This can create significant vulnerabilities and allow threat actors to move easily between systems. In the event a device is compromised, adversaries can easily move laterally if proper measures are not put in place.system and keep it updated with all patches.

Here are some network security best practices:

- It is advisable for an IT or security team to restrict communications using host-based firewall rules to deny the flow of packets from other hosts in the network. Implementation of firewall rules can be created to filter on a host device, user, program, or internet protocol (IP) address to limit access from services and systems.
- Security teams are also advised to implement a VLAN access control list (VACL) which serves as a filter to control access to and from VLANs. VACL filters should be created to deny packets the ability to flow to other VLANs.

Another important aspect of network security is safeguarding networking devices with secure configurations. Here are some best practices:

- Disable unencrypted remote admin protocols used to manage network infrastructure [i.e. Telnet, File Transfer Protocol (FTP)].
- Disable unnecessary services such as discovery protocols, source routing, hypertext transfer protocol (HTTP), simple network management protocol (SNMP), and bootstrap protocol.
- Use SNMPv3 or a subsequent version.
- Secure access to the console, auxiliary, and virtual terminal lines.
- Implement robust password policies and use the strongest password encryption available.
- Protect routers and switches by controlling access lists for remote administration
- Restrict physical access to routers and switches.
- Back up configurations and store them offline.
- Use the latest version of the network device operating
- Periodically test security configurations against security requirements.

WIRELESS SECURITY

A wireless local area network (WLAN) is defined as a group of wireless networking devices within a limited geographic area—such as an office building—that exchange data through radio communications.

WLAN's often consist of laptops, smartphones, and access points which connect devices with a distribution system—typically the organization's wired network infrastructure. WLANs also use wireless switches, which act as intermediaries between access points and the distribution system.

The security of each WLAN is often dependent on how well each WLAN component—including client devices, APs, and wireless switches—are secured throughout. This is relevant from initial WLAN design and deployment through ongoing maintenance and monitoring. Unfortunately, WLANs are typically less secure than their wired counterparts for several reasons, including ease of access and weak security configurations often used for WLANs.

For WLANs requiring wired network access, client devices should be configured to only allow access to the necessary hosts on the wired network, which involves only the required protocols. It is also advisable to have separate WLANs if there is more than one security profile for user groups—for example, separating WLANs for external use (guest Wi-Fi) and internal use. Devices on one WLAN should not be able to connect to devices on a logically separated WLAN.

Security monitoring is important for all systems and networks, but it is generally even more important for WLANs because of the increased risks that they face. Organizations should continuously monitor WLANs for WLAN-specific and network based attacks. To best mitigate the risk associated with WLANs, organizations are encouraged to identify patches and apply them in a timely manner. These actions should be performed at least as often for WLAN components as they are for the organization's remaining infrastructure.

REMOTE ACCESS

Secure remote access touches just about every aspect of security. As the concept of the perimeter quickly fades, securing the edge is an emerging concept that combines network and security functions into a cloud service. Many organizations have moved in this direction to embrace a remote workforce, IoT adoption, and cloud-based application use.

The following technologies are investments that can contribute to secure remote access:

- VPNs
- Intrusion Prevention Systems & Intrusion Detection Systems (IPS/ IDS)
- Secure Access Service Edge (SASE)
- A Software-Defined Perimeter
- Firewalls
- Cloud Access Security Brokers
- Zero Trust Network Access
- Virtual Desktop Infrastructure
- Identity & Access Management (IAM).

CYBERSAFE SOLUTIONS®

MANAGED DETECTION & RESPONSE (MDR)

Managed detection, response, and containment (MDR) is a cybersecurity service that combines technology and human expertise to perform proactive threat hunting, continuous security monitoring, and real-time response. By investing in the proper MDR solution, businesses can detection and eradicate threats in real time without the need for additional staffing.

Organizations using an MDR solution are empowered with live detection of cyber events. Without such visibility, the typical detection time is nearly 280 days and is generally noticed after irreversible damage has occurred.

However, reducing detection time from months to mere minutes is not the only benefit. Organizations can also:

- Improve Security Posture
- Identify & Isolate Sophisticated Threats Evading Traditional Anti-Virus
- Detect Vulnerabilities With Proactive Threat Hunting
- Respond to Threats More Effectively Through Guided Response & Managed Remediation
- Allow Staff to Focus Only Threats Requiring Attention, Rather Than Sift Through Noise

When scoping out an MDR provider, it is important to distinguish between providers and the tools themselves. MDR tools are often noisy and can result in alert fatigue for teams without additional staffing. Determining the appropriate response to events in these platforms is critical. When purchasing a tool, these alerts can require more management and expertise than is typically retained in-house. By contacting the appropriate provider for your organization, you can ensure it will be an extension of your team—allowing you to get the most out of your investment.

NETWORK VULNERABILITY & PENETRATION TESTING

A penetration test is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries.

These tests take the point of view of an attacker and see how resistant your infrastructure may be if it were breached by a dedicated adversary. This is an essential component of an overall information security strategy and should be conducted once an organization has mitigated security gaps. When performed at the right time, penetration testing takes the concept of "what if" to reality, with the goal being: The more difficult it is for a tested hacker, the more difficult it is for a legitimate threat actor.

However, not all penetration tests are created equal. These assessments range in scope, investment and number of resources dedicated to the project—which also results in varying budgets.

It is equally important to address the findings of a penetration test, but as penetration tests are only a point in time, even satisfactory results should not provide a false sense of security. Continuous vulnerability management can identify new security gaps between annual testing, and proactive threat monitoring also detects if a threat actor exploited any weak points.

CYBER RISK INSURANCE

Closing the threat gap is done by implementing reasonable and appropriate preventative tools; while also having visibility to detect, respond, and contain threats as they happen; and lastly, transferring any remaining risk to an insurance policy.

CYBERSAFE SOLUTIONS®