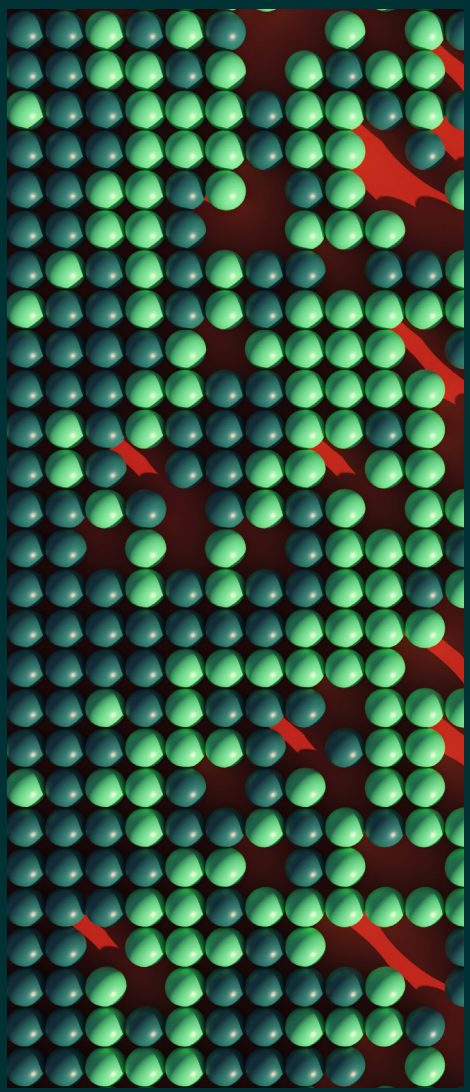
unisys

A new urgency for cyber resilience

Cybersecurity Solutions from Unisys



Cyber attacks such as ransomware, denial of service and data breaches pose significant threats to the security, reputation and continuity of any organization.

According to the 2024 Verizon Data Breach Investigations Report, roughly one-third of all breaches involved ransomware or some other extortion technique.

In one recent analysis, publicly traded companies suffered an average decline of 7.27% share price drop following the breach, with financial and technology companies impacted the greatest. The damage to reputation and trust stemming from a disclosed breach can result in a credit rating downgrade, impacting a company's ability to secure financing. In fact, Moody's announced in 2018 that it would evaluate companies' cybersecurity practices when assigning credit ratings. As a result, companies with weaker cybersecurity practices may face higher borrowing costs and increased financial risk.

Most regulated industries now have mandates that require companies to have a cyber resiliency plan in place, and many governments (the United States, Australia and the European Union) have directives in place or in draft form.

Given the increasing number of ransomware attacks and their detrimental effects on businesses and individuals alike, building and maintaining an effective cyber resilience program that can prevent, detect and respond to these threats has become essential.

Building blocks of an effective cyber resilience strategy

Minimizing the impact of inevitable security incidents requires strengthening cyber defenses with the right tools, processes and strategies. Key characteristics of an effective cyber resilience program include:

Best practices

Any enterprise that deals with data or has an online presence needs a compliance program to ensure they meet standards set by authorities to protect information's confidentiality, integrity and availability. An effective compliance program focuses on implementing risk-based controls to safeguard data at every stage, whether stored, processed, integrated or transferred.

Understanding your government's major cybersecurity regulations and identifying the correct cybersecurity regulations needed for a business or industry is important. An effective compliance program is based on standards such as the NIST Cybersecurity Framework, ISO 27001 and CIS Benchmarks, all created to help organizations manage their particular risk.

Subject matter expertise

Qualified security professionals with real-life experience can help plan, manage and execute cyber resilience programs. These professionals should have the skills and knowledge to assess cyber risks, design and implement security policies and controls, monitor and analyze security events and respond to incidents effectively. An effective security expert should also have the skills to communicate and collaborate effectively with stakeholders, vendors, regulators and customers on cybersecurity matters.

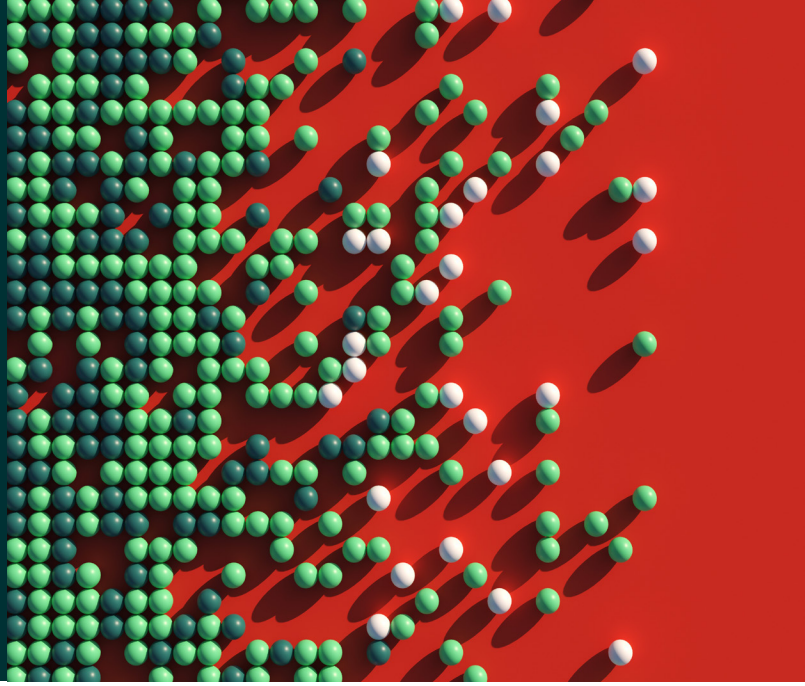
State-of-the-art technologies

New technologies, such as anti-ransomware solutions, encryption, backup and recovery processes, endpoint protection, firewalls, micro-segmentation, immutable storage, antivirus scans and software, and network monitoring, can enhance cyber resilience capabilities. These technologies help prevent or mitigate the impact of cyber attacks, protect the data and systems from unauthorized access or modification and quickly restore normal operations in case of a disruption.

Cyber resilience:

The ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources

Control what you can



While no one can predict where or when a ransomware attack might be detonated, Cybersecurity Solutions from Unisys can help organizations control and protect what they can by implementing these attributes in a cyber recovery solution:

Security awareness training

Develop a culture of security that helps manage the biggest cybersecurity threat: human error. Many ransomware attacks begin with phishing that exploits the tendency of staff to open email attachments or click on links that then install rogue software. Providing frequent security awareness training and incentives for maintaining security awareness is highly effective as a first line of defense.

Expert consulting

Unisys cybersecurity experts take time to understand your business and guide designing, implementing and managing a cyber recovery solution. These experts can assess the current cyber resilience posture, identify the gaps and vulnerabilities, recommend the best practices and technologies and assist with the deployment and configuration of the solution. For example, updating or creating a living information security policy requires a security expert well-versed in evolving threats and the importance of complex regulatory and data privacy compliance.

Endpoint fortification

Endpoints serve as the primary gateway for cyber attacks. Research suggests that up to 90% of effective cyber attacks and 70% of successful data breaches stem from activities originating at endpoint devices. Properly managing endpoints and implementing Zero Trust strategies shields against external and internal threats, even for connections already within the network.

Border security

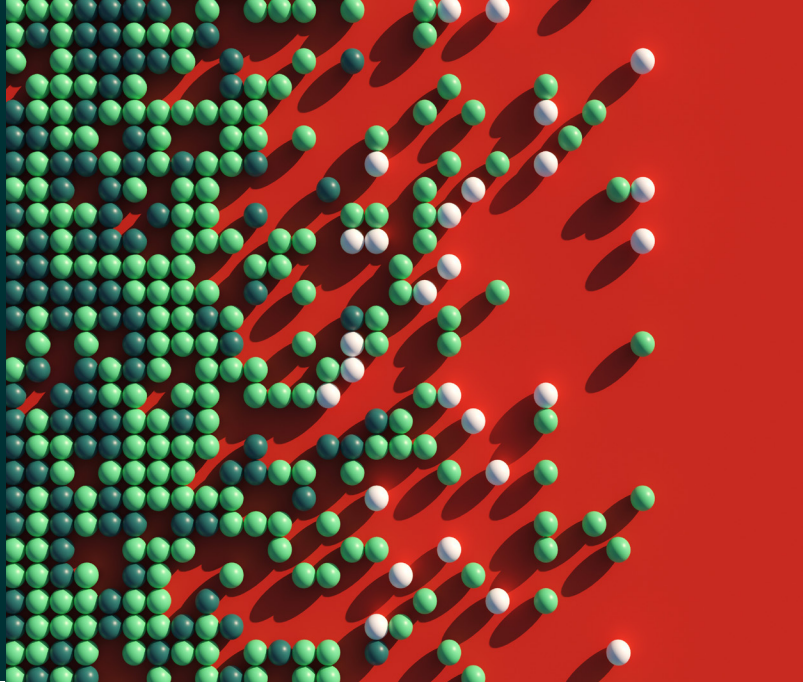
To ensure your attack surface is as small as possible, deploy appropriate security technologies, such as multi-factor authentication, and ensure that your organization keeps all vulnerability patches current.

Moody's calls cyber attack on MGM "credit negative"

Moody's Investor Service stated that the recent data breach at MGM highlighted risks related to the company's heavy reliance on technology and the operational disruption caused when systems needed to go offline. Additional risks included reputational damage and costs related to investigation and remediation.

Control what you can

(continued)



Anti-ransomware technologies

These technologies help prevent or stop ransomware attacks by detecting and blocking malicious files or processes, isolating the infected devices or networks and alerting the security team. Anti-ransomware technology also helps recover ransomware-encrypted data by restoring it from a clean backup or decrypting it with a key. Unisys works with advanced anti-ransomware technologies that prevent crypto-locking of your systems and data.

Cyber recovery vault

This vault is a secure, access-controlled and isolated storage environment that can protect critical data and systems from cyber attacks. The vault can store an immutable copy of the backup data, which can undergo machine learning-powered integrity checks, and systems that only authorized users can access. Depending on the existing infrastructure, a vault can be located on-premises, adjacent to the cloud or in the cloud. The data and applications stored in the vault can also be restored to a secure computing area to demonstrate that the backups are valid and ensure that recovery can be achieved quickly.

Managed services with 24/7 monitoring and updates

This service provides continuous visibility and awareness of the organization's security status. Security compliance is not static, and a dedicated team is required to stay ahead of any threat. The service ensures that vulnerability patches are installed, monitors security events and alerts with server and mobile device management, analyzes the threats and risks and notifies the security team to take action if needed.

The Unisys Cyber Recovery solution can help an organization improve its cyber resilience by:

- Reducing the likelihood of a successful cyber attack by preventing or blocking ransomware or other malicious activities
- Minimizing the impact of a cyber attack by isolating or containing the infection or damage
- Accelerating the recovery from a cyber attack by restoring or recovering the data and systems from a secure vault
- Enhancing the confidence and trust of stakeholders, vendors, regulators and customers by demonstrating a strong commitment to cybersecurity

Insure what you can't

Ransomware insurance may limit the cost or financial exposure of an attack but may not entirely address the recovery. Additionally, premiums have increased with the proliferation of attacks, and many insurers are beginning to refuse payment, with 27% of claims containing exclusions. With the average insurance payout totaling $812,360 and the average cost of a ransomware attack costing $4.54M, there is a clear imperative for organizations to implement cyber-resilient systems to ensure confidentiality, integrity and availability of infrastructure, networks, systems and applications. Think of cyber recovery technology as both a preventative measure and an insurance policy that will lessen your exposure and lower the effort and costs of recovery.

Complying with industry regulations to mitigate risk

The Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. has identified 16 critical industry sectors that need special protection due to their potential impact on national security, the economy, public health and safety.

Next steps

Investing in a cyber resilience program is important in today's digital landscape, where cyber attacks pose significant threats to an organization's security, reputation and continuity. The increasing frequency and severity of ransomware attacks underscore the urgency of implementing an effective cyber resilience program.

To learn more about how Cybersecurity Solutions from Unisys can benefit your organization, visit us online or contact us today.

unisys

unisys.com

11/24 3630-7663