VTC

13 TIPS FOR MODERATING CYBERATTACKS & PROTECTING DATA

Cybersecurity & Fraud Protection

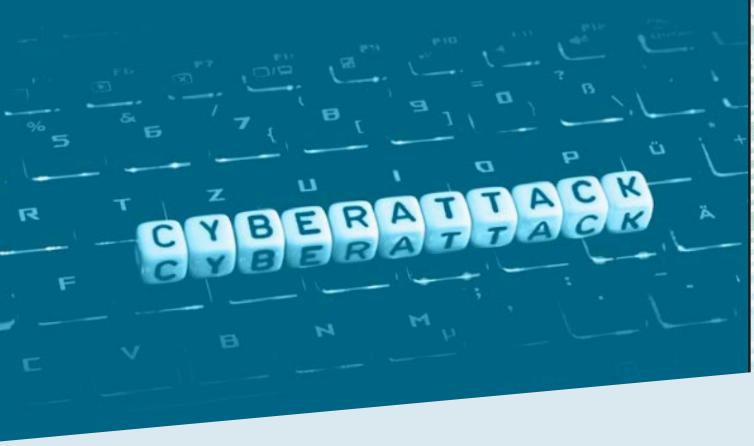
These thirteen cybersecurity strategies can serve as a foundation for your mitigation plan and strengthen your organization's security protocols.

1. Renew and Upgrade Software

Apply all software updates as soon as they are available. Cybercriminals can engineer exploits almost as quickly as a patch is made, so enable automated updates if possible. Be sure to use updates delivered through protected links and to assess them prior to production release.

2. Restrict and Control Account Access

Threat actors gather account credentials, so it is suggested that you begin your program with a zero-trust basis. Under this model, account privileges are assigned only as users need them. Lingering profiles can be a problem, so proactively shut down control and access to current and former employees who no longer need them. Likewise, update your onboarding, internal transfer and offboarding procedures to align with a zero-trust approach. You should also document procedures for securely resetting credentials. Consider using a privileged access management tool to automate credential management. Human Resources will set the policy, and IT will execute the policy.



3. Implement Signed Software Execution Policies

Allowing unsigned software can give cybercriminals an entry point, so it is critical to enforce signed software execution policies, so devices use the most up to date, verified versions available. You can protect your operating system with a protected boot – a capability that ensures devices boot using only secure software.

4. Create a Disaster Recovery Plan

Crafting an evergreen disaster recovery plan (DRP) is key to efficiently mitigating cyberattacks. Start your DRP by detecting essential functions to ensure business continuity, then craft your plans to help mitigate interferences to your business and technology. Remember, a DRP is not a static document; always review, evaluate, and update your plan. Developing periodic reviews into your overall cybersecurity risk management plan can help recognize any gaps.

5. Actively Oversee Systems and Configurations

Regularly scan and take inventory of your network devices and software. Revitalize your network security configuration as needed and eliminate redundant hardware and software from the network. This method can help you mitigate cyber risk by reducing the attack surface and establishing control of the operational environment.

6. Search for Network Intrusions

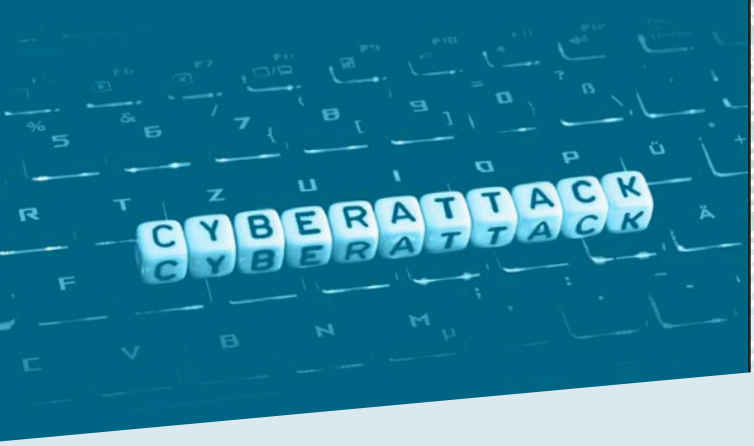
Operate under the assumption that a compromise has ensued and take initiative-taking measures to detect, contain, and remove any malicious presence. Automated tools, such as endpoint-detection and response solutions, must be paired with hunt operations and penetration testing. Such steps can shift your cybersecurity defense strategies from basic detection and remediation.

7. Leverage Hardware Security Features

Computers' built-in hardware contains security features that can improve system integrity. Schedule a hardware refresh for older devices, or at minimum use an updated operating system on outdated hardware. This can help better protect systems, critical data, and user credentials from threat actors.tsoftware.

8. Segregate Networks Using Application-Aware Defenses

Cybercriminals can compromise your data by hiding malicious activity over common procedures that transfer data across networks. Application-aware mechanisms, such as firewalls, can contain certain applications if they are compromised. Start by isolating critical networks and services, then implement network defenses to block malicious traffic and content.



9. Consider Using Threat Reputation Services

Cyberthreats develop rapidly – often faster than organizations can manage – so consider using threat reputation services. There services can scan for emerging threats in real time to advance your coverage.

10. Leverage Multifactor Authentication

Multifactor authentication is a necessity for mitigating cyberattacks. Use this protection for accounts with advanced privileges, remote access, and high-value assets. Use physical, token-based authentication systems to supplement knowledge-based factors, such as passwords and PINs.

11. Monitor Third-Party Security Position

Vendors, third-party suppliers, and clients present a unique set of security risks. External partners often have access to your organization's sensitive data or support essential business processes. It is critical that you constantly monitor third-party risks and accurately assess partner cybersecurity plans to help secure your assets. Request assessments on a recurring basis and obtain compliance attestations annually.

12. Assume Insider Threats Exist

Insider threats occur in various forms, ranging from intentional misuse of system access and confidential information to inadvertent errors, such as clicking on a phishing email. Consider adopting a layered approach for addressing insider threats, including regular assessments and ongoing employee training and awareness campaigns. Automated tools, such as endpoint-detection and response solutions, must be paired with hunt operations and penetration testing. Such steps can shift your cybersecurity defense strategies from basic detection and remediation.

13. Cyber Insurance

As cyberattacks become more frequent and costly, it's crucial for organizations to maximize their financial protection against related losses by purchasing sufficient insurance. Cyber coverage, or cyber liability insurance, can help businesses pay for a range of expenses that may result from cyber incidents – including data breaches, ransomware attacks, and phishing scams. Specific cyber insurance offerings differ between carriers. Organizations' coverage needs may vary based on their exposures. Cyber insurance agreements typically fall into two categories: first-party coverage and third-party coverage.

First-Party Coverage

First-party cyber insurance can offer financial protection for losses that a corporation directly sustains from a cyber incident. Covered losses generally include the following:

- **Incident Response Costs** – This coverage can help pay the costs connected with responding to a cyber incident. These costs may include using IT forensics to examine the breach, restore damaged systems, notify affected customers, and set up call-center services.
- **Legal Costs** – This coverage can help pay for legal counsel to assist with any notification or regulatory responsibilities resulting from a cyber incident.
- **Data Recovery Costs** – This coverage can help recover expenses related to reconstituting data that may have been deleted or corrupted during a cyber incident.
- **Business Interruption Losses** – This coverage can help reimburse lost profits or additional costs incurred due to the unavailability of IT systems or critical data amid a cyber incident.
- **Cyber Extortion Losses** – This coverage can help pay costs associated with hiring extortion response specialists to evaluate recovery options and negotiate ransom payment demands (if applicable) during a cyber incident.
- **Reputational Damage** – This coverage can help pay for crisis management and public relations services related to a cyber incident.

Third-Party Coverage

Third-party cyber insurance can provide financial protection for claims made, fines incurred, or legal action taken against an organization due to a cyber incident. Types of third-party coverage usually include the following:

- **Data Privacy Liability** – This coverage can help recover the costs of dealing with third parties who had their information compromised during a cyber incident. These costs may include handling third-party lawsuits or legal disputes, offering credit-watch services and providing additional compensation.
- **Regulatory Defense** – This coverage can help pay fines, penalties and other defense costs related to regulatory action or privacy law violations stemming from a cyber incident.
- **Media Liability** – This coverage can help reimburse defense costs and civil damages resulting from defamation, libel, slander, and negligence allegations associated with the publication of content in electronic or print media. Multimedia liability coverage can also offer protection amid copyright, trademark, or intellectual property infringement incidents.

Questions? Contact your VTC Representative today.

VTC INSURANCE GROUP

Confidence. *For What's Next.*®

248.828.3377 www.vtcins.com