RECAST SOFTWARE

Cybersecurity Assessment for IT Leaders

Companies must do more than meet minimum security requirements. With the rapid evolution of threat strategies, organizations must also evolve and implement best-practices to protect their assets and information.

To prepare for cybersecurity insurance vendor meetings or current insurance audits, use this assessment to evaluate your organization's cybersecurity posture and how well it aligns with common requirements for securing insurance coverage.

Security Policies and Procedures

Authentication and Access Control

Multi-Factor Authentication (MFA)

- [ ] Is MFA implemented for all employee accounts?
- [ ] Are multiple forms of verification used (e.g., something the user knows, has, or is)?
- [ ] Is MFA enforced for both on-premises and remote access?

Single Sign-On (SSO)

- [ ] Is SSO implemented to simplify the authentication process while maintaining security?
- [ ] Are SSO activities logged and monitored for suspicious behavior?

Privileged Access Management

- [ ] Does your company use least-privilege access tools?
- [ ] Does your network block lateral movement (micro segmentation)?

Data Protection

Comprehensive Backup Strategy

- [ ] Are all critical data and systems backed up?
- [ ] Are backups stored off-site, separate from the main network?
- [ ] Is there a defined schedule for creating and testing backups?

Encryption of Sensitive Data

- [ ] Is data at rest encrypted?
- [ ] Is data in transit encrypted?

Network Security

Implementation of Zero Trust Principles

- [ ] Does your organization treat all devices as potential breach points?

Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR)

- [ ] Is an EDR or MDR solution in place to monitor all endpoints?
- [ ] Is the solution configured to send real-time alerts for suspicious activities?
- [ ] Is there a process for quickly isolating affected endpoints to minimize the spread of an attack?

Employee Training

Security Awareness Training and Testing

- [ ] Is security training required on a regular basis, such as quarterly or semi-annually?
- [ ] Is there a security awareness training program in place?
- [ ] Are all employees required to complete this training?
- [ ] Is the training updated to cover the latest cybersecurity threats and trends?
- [ ] Are simulated attacks (e.g., phishing tests) conducted to test employee awareness?
- [ ] Are training modules tailored according to job roles?

Risk Management

Regular Risk Assessments

- [ ] Does your company regularly do assessments of the network, data, people, and devices to classify your risk levels?
- [ ] Are the outcomes of the risk assessments reviewed by upper management?

Vulnerability Management

Patch Management

- [ ] Are new patches systematically or automatically identified within 48 hours, either using internal resources or using third-party software tools?
- [ ] Does patch monitoring include third-party software update monitoring?
- [ ] Is there a system in place to prioritize patches based on the severity of the vulnerabilities they address?
- [ ] Is there a documented process for how patches are tested before being deployed?
- [ ] Are all patching activities logged and are these logs reviewed regularly?

Vulnerability Scanning and Assessment

- [ ] Is there a process for regularly identifying security vulnerabilities in systems and applications?
- [ ] Are regular scans and assessments conducted to identify vulnerabilities?
- [ ] Is there a timeline and responsibility matrix for patching known vulnerabilities?
- [ ] Do you regularly review your hardware and software to ensure they are not outdated or unsupported, as the use of legacy systems may disqualify you from insurance coverage in the event of a cyberattack?

Security Information and Event Management (SIEM)

- [ ] Is a SIEM solution in place to correlate logs and generate alerts based on predefined conditions?
- [ ] Does your SIEM solution have a defined log retention policy that complies with regulatory requirements?
- [ ] Is the SIEM solution integrated with your incident response plan to accelerate containment and mitigation strategies?
- [ ] Do you have staff trained specifically to manage and interpret SIEM data?
- [ ] How frequently are SIEM configurations and alert thresholds audited for effectiveness?
- [ ] Is the SIEM solution configured for real-time monitoring of security events?

RECAST SOFTWARE

Industry Specific Compliance Standards

Examples

- [ ] General Data Protection Regulation (GDPR)
- [ ] Health Insurance Portability and Accountability Act (HIPAA)
- [ ] Payment Card Industry Data Security Standard (PCI DSS)

Incident Response Plan

Incident Detection and Response

- [ ] Is there a documented incident response plan?
- [ ] Does the plan outline roles, responsibilities, and procedures for responding to a cyberattack?
- [ ] Is the plan regularly reviewed and tested to ensure its effectiveness?
- [ ] Do you have automated alerting for specific types of incidents?
- [ ] Is there a defined sequence of steps for containing an incident?

Communication Strategies

- [ ] Is there a communications protocol, including a list of internal and external contacts?

Post-Incident Analysis

- [ ] Is there a process for conducting a post-mortem analysis after an incident has been handled?

Utilize this checklist as a part of your cybersecurity insurance planning. By completing this assessment, you'll be well on your way to demonstrating your commitment to IT security, making you an attractive candidate for cybersecurity insurance and a more secure company.

RECAST SOFTWARE

How Recast Software Helps You Meet Cybersecurity Insurance Requirements

APPLICATION MANAGER

Maintaining up-to-date software is vital for security and mandated by most insurers as part of vulnerability management protocols. Application Manager streamlines the application patching and updating process, notifies you in real-time about essential updates or patches, and mitigates vulnerabilities that could otherwise expose your systems. It takes the burden off your patch teams and reduces the scope for human error.

RIGHT CLICK TOOLS

Streamlining OS and manufacturer updates (Dell, Lenovo firmware, etc.) updates is crucial for maintaining a secure environment. Right Click Tools assist in locating devices behind on their updates and offers insights on update failures. It empowers IT teams to kick off updates remotely, reducing time and resource consumption. Incorporating Right Click Tools into your IT operations can significantly bolster your EDR or MDR capabilities.

PRIVILEGE MANAGER

The weakest link in cybersecurity often turns out to be fallible humans. Privilege Manager limits user permissions to essential functionalities, thereby mitigating risks such as unauthorized software installations or dangerous clicks. This is particularly valuable when aiming for the highest standard in security awareness among your staff.

Incorporating these solutions from Recast Software will make you a more secure and attractive candidate for cybersecurity insurance, while also helping you score better on your cybersecurity assessment. Reach out to learn more.