



Advisory



Organizations



Cybersecurity

# How internal audit can fortify cybersecurity

January 25, 2022

When you're trying to stay a step ahead of ransomware attackers, adjusting your organization's cybersecurity profile can start to seem like an endless game of whack-a-mole.

As ransomware threats expand, internal audit leaders can play a vital role in delivering value-driven insights that help management and the audit committee understand the organization's cybersecurity risks, resilience and potential for recovery.

Ransomware attacks can be launched from undetected software vulnerabilities, or when an employee opens a phishing email and clicks a link that unleashes malicious software. Such software can cut to the core of business operations and drive companies to pay multi-million-dollar ransoms.

## The role of internal audit

As cybercrimes accelerate, a crucial role has evolved for internal audit. Internal audit must help their organization anticipate, adapt, and respond to these attacks against a backdrop of faulty or neglected systems and practices. Four critical areas often provide openings for these attacks:

- **cybersecurity resilience:** as the list of threats grows, the maturity of cybersecurity resilience often fails to keep pace.
- **third-party ecosystems:** companies are expanding their reliance on third parties, entrusting them with greater access to organizational data and critical tasks, while monitoring and lifecycle management of third parties has often lagged.
- **advanced technology solutions:** the march of automation, data-rich production cycles and the use of third parties make entire industries vulnerable to cyberattacks.
- **data governance:** few organizations have a formal and mature governance framework in place to enforce data classification, lifecycle management and technology solutions.

## The larger question of resilience

Overall cybersecurity resilience is a critical factor in defending against ransomware attacks. It requires organizations to prepare for impacts from cyberattacks that cannot be predicted or prevented. It also requires close collaboration with third-party service providers, intelligence agencies, industry groups, security analysts, customers, and supply chains.

The key elements of cybersecurity resilience include:

- **governance:** this includes building collaborative communities and intelligence sharing, assessment, and validation, defining and enforcing roles and responsibilities, promoting accurate reporting, and making informed decisions.
- **detective and protective controls:** some examples of controls are user access reviews, strategic system segmentation and user integrity assurance. These follow the principle of least privilege, ensuring that access is aligned to the minimum access needed to perform a job.
- **technical capability with optimized controls:** this calls for ensuring that the standard response processes to an attack become the minimum acceptable level; reviewing changes in technology; tracking, logging, and alerting; and testing the controls through the use of adversary emulation.
- **response and recovery:** it is essential to regularly update incident response plans, train users based on current threats, and build resilience recovery based on the standard recovery processes of backup, disaster recovery and continuity planning.

### The evaluation of evaluations

To form a coordinated defense, organizations must ensure that their technical controls stay updated and effective across a range of factors. Internal audit can play an invaluable role in evaluating the risk landscape, communicating the impact of a risk materializing, performing technical audits aligned to changing risks, reviewing cybersecurity insurance coverage and ensuring board-level reporting.

One effective way to evaluate technical controls is by using a risk-based framework. Internal audit can leverage comprehensive standards such as these standards and others in the NIST 800 series provide practical guidance on how to address tangible risks with technical controls:

The infographic consists of four grey rectangular boxes arranged in a 2x2 grid. Each box features a purple circular icon at the top center, a title in bold purple text, and a list of risk, standards/frameworks, and technical capability elements in black text.

- Remote access security** (Icon: Laptop):
  - Risk**
    - Risk of remote access communications being carried over untrusted networks and exploitation of remote access client devices
  - Standards / frameworks**
    - NIST SP 800-46
  - Technical capability elements:**
    - Tracking anomalous behavior for potential insider threat given the fluid workforce
    - Balancing performance demands (like VPN outage) for increased remote workforce
- Privileged access management** (Icon: Network nodes):
  - Risk**
    - Risk of potential misuse of privileged accounts being a constant target of malicious actors as they look to infiltrate valuable information or cause damage to an organization
  - Standards / frameworks**
    - NIST 800-53
  - Technical capability elements:**
    - Monitoring high level of activity for privileged users
    - Monitoring violations for principle of least privilege
- Protecting the PII / PFI / PHI** (Icon: Smartphone):
  - Risk**
    - Risk of PII being lost, stolen, or compromised, and the potential that the information is being used or may be used for unlawful purposes such as identity theft or fraud
  - Standards / frameworks**
    - NIST SP 800-122
  - Technical capability elements:**
    - An introduction to PII and the fair information practices
    - Methods for protecting the confidentiality of PII that can be implemented to reduce PII exposure and risk
- Enterprise patch management** (Icon: Shield with checkmark):
  - Risk**
    - Risk of inadequate patch management leaving loopholes in the IT infrastructure leading to cyber attacks
  - Standards / frameworks**
    - NIST 1800-31
  - Technical capability elements:**
    - Overcoming common obstacles involving enterprise patching for general IT systems
    - Achieving a comprehensive security hygiene program based on existing standards, guidance, and recommended practices

### The plan to respond

When internal audit stays up to date with cybersecurity trends and leading practices, it is well-positioned to independently monitor an organization's cybersecurity resilience, recommend how the organization can mature its program and update its incident response plan.

There are several opportunities for internal audit to enhance incident response plans.

- **guidance:** internal audit can provide guidance on a plan that is aligned with cybersecurity policy and procedures while also being easier to implement and monitor.
- **templates and playbooks:** internal audit can help ensure these are customizable and come preconfigured to automate multistep responses.
- **tools:** internal audit can help identify tools to assist teams in responding to a greater number of increasingly sophisticated attacks on increasingly complex systems.

### The test

Internal audit leaders know that organizations need to go on the offensive by aggressively testing their defensive measures. Many use the following advanced approaches in tandem:

- **proactive cybersecurity assessment:** this evaluates an organization's environment for the presence of attacker activity, using tools like CrowdStrike to search for signs of compromise, technology hygiene issues and lack of controls.
- **adversary emulation assessment (AEA):** this is a controlled execution of a security test that mimics a real-world cyberattack to test the effectiveness of technical controls. It is different from a penetration test because it focuses on specific threat-actor tactics and control areas.



In tandem, these approaches add value by providing robust insights into cybersecurity control risks, system hygiene and potential exposures. They also afford deeper, more focused testing and yield recommendations that help defend against intrusions and respond to threats.

Grant Thornton library articles:

[How internal audit can fortify cybersecurity](#)

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for assistance in relation to this or any other matter, we will be glad to assist you.



**Marta Rodríguez**  
Partner Head of Advisory  
E [marta.rodriguez@pr.gt.com](mailto:marta.rodriguez@pr.gt.com)



**Neysha Otero**  
Advisory Manager  
E [neysha.otero@pr.gt.com](mailto:neysha.otero@pr.gt.com)



**Jorge Paredes**  
Advisory Manager  
E [jorge.paredes@pr.gt.com](mailto:jorge.paredes@pr.gt.com)



**Jorge Oquendo**  
Advisory Manager  
[jorge.oquendo@pr.gt.com](mailto:jorge.oquendo@pr.gt.com)



[grantthornton.pr](http://grantthornton.pr)

DISCLAIMER: This update and its content do not constitute advice. Clients should not act solely on the basis of the material contained in this publication. It is intended for information purposes only and should not be regarded as specific advice. In addition, advice from proper consultant should be obtained prior to taking action on any issue dealt with this update. Information provided in this publication may change in the future and such change may be applied retroactively. Kevane Grant Thornton LLP does not assume the responsibility to update this communication if the applicable laws change.

© 2022 Kevane Grant Thornton LLP All rights reserved. Kevane Grant Thornton LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. Please visit [www.grantthornton.pr](http://www.grantthornton.pr) for further details.