MANAGING CYBERSECURITY RISK

An Internal Audit Perspective

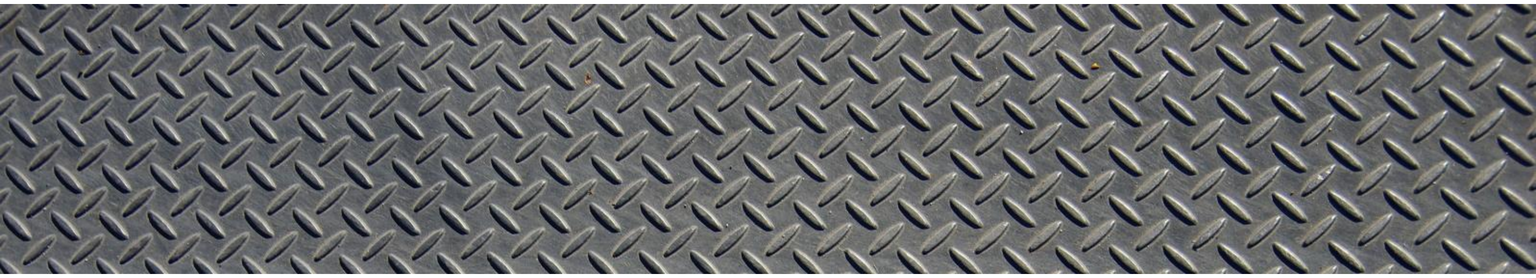
INNOVATE. TRANSFORM. SUCCEED.

Adapt to the new business reality.

protiviti®

Face the Future with Confidence

TABLE OF CONTENTS



IS CYBERSECURITY IMPORTANT?

Ask a business leader if cybersecurity is important and you will hear a resounding

"YES."

Businesses have long known that cybersecurity is important but the exponential advancement of technology and ever evolving privacy landscape continues to underscore the importance of knowing what data is being captured and how it is stored, used and secured.

Board members and C-Suite executives worldwide continue to call out cybersecurity, data privacy, and regulatory matters as "long-term concerns" according to Protiviti and North Carolina State University's ***2022 and 2031 Executive Perspectives on Top Risks*** survey.

In fact, the survey ranked "cyber threats" as ninth in the top ten risk concerns for 2022 and found that organizations continue to focus on how these threats might interrupt core operations and erode brand image.

✚ Read the full report at protiviti.com/TopRisks

BUT, WHAT DOES CYBERSECURITY MEAN?

Cybersecurity and *cyber threats* are vague terms that can interpreted broadly.

So, let's try to focus in on the cybersecurity risks that are most relevant to Technology professionals. ISACA and Protiviti's 10th Annual ***IT Audit Technology Risks Survey*** also support the conclusion that cybersecurity, privacy, data and regulatory compliance are top-of-mind concerns.

This global survey of more than 7,500 IT audit leaders and professionals from around the world reveals a dynamic threat landscape that includes the following Top 10 technology risks:

1. **Cyber Breach** – Vulnerability to cyber incidents that could result in the compromise or disruption of data or systems that have a significant impact on business activities.
2. **Manage Security Incidents** – Security incidents are not Identified, classified, routed, and tracked to completion. Monitoring and escalations are not defined or effective to ensure incidents are appropriately prioritized and resolved on a timely basis to ensure meeting service requirements and adequately respond and recover systems from attacks and compromises.

✚ Read the full report at
protiviti.com/ITAuditSurvey

TOP 10 TECHNOLOGY RISKS

3. **Privacy** – The organization lacks sufficient controls and oversight of its data and compliance with privacy regulations.
4. **Monitor Regulatory Compliance** – Processes and controls are inadequate to identify new compliance requirements and changes to ensure they are addressed in a timely basis to meet compliance requirements. There is a lack of monitoring ongoing compliance and reporting
5. **Access Risk** – The organization's access to information or systems will be inappropriately granted or refused. This includes the risk of improper segregation of duties, risks associated with the integrity of data and databases, and risks associated with information confidentiality.
6. **Data Integrity** - There is lack of clarity with regard to the authorization, completeness and accuracy of transactions and other data as they are entered into, processed by, summarized by and reported on by the various application systems deployed by an organization.
7. **Disaster Recovery** - The organization lacks a comprehensive and documented disaster recovery plan for IT that could result in an extended disruption of IT services and performance.
8. **Data Governance** - The organization lacks sufficient processes to ensure critical data assets are defined, and lacks a sufficient structure for cleansing, storing and reporting data in a way that makes it easy for the business to own and identify variances in its mission-critical information.

EMERGING SECURITY TRENDS

> “Even the bravest cyber defense will experience defeat when weaknesses are neglected.”
>
> Stephane Nappo
> Global Head Information Security
> Société Générale International Banking

Many organizations already have controls in place to mitigate these risks in many of their technology environments, but there are several emerging trends where these risks are more commonly exploited.

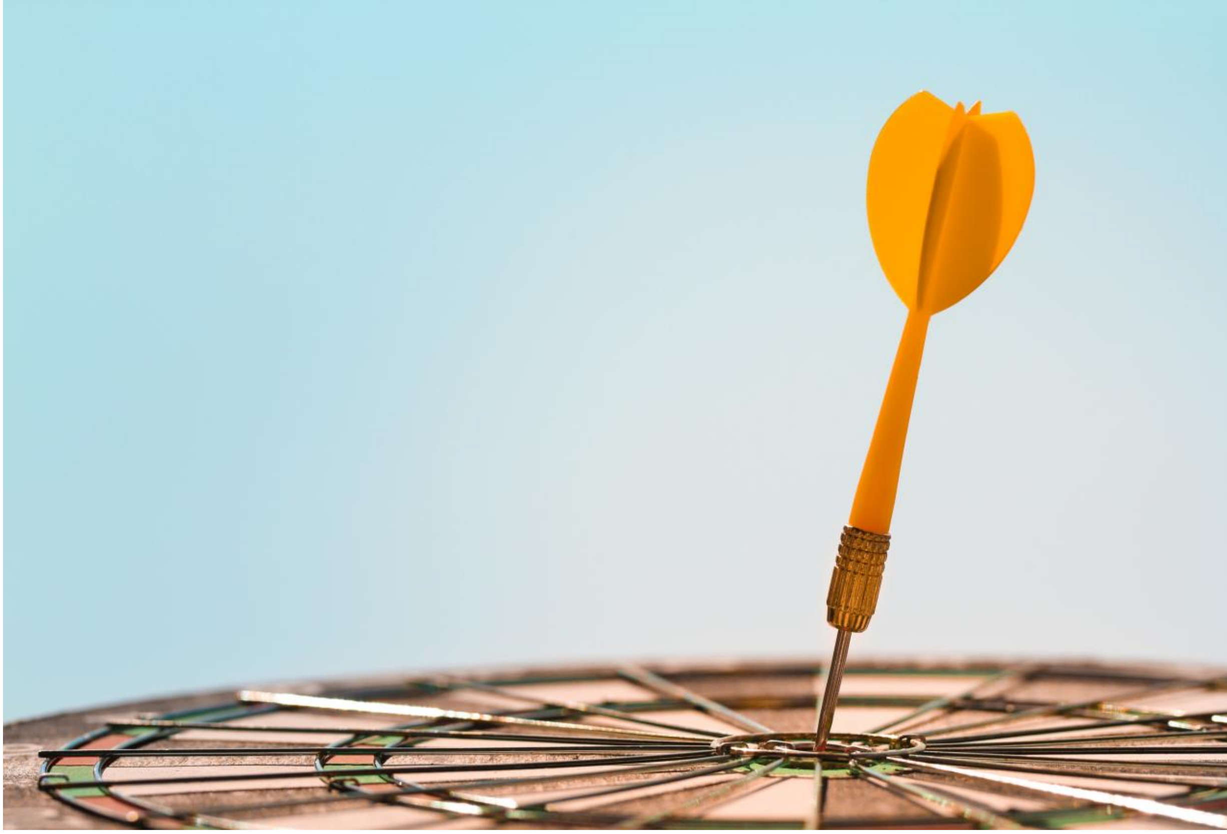
CLOUD: The use of cloud has increased, necessitating the need for security measures to be put in place to avoid a data breach.

REMOTE WORK: During remote working, an organization must identify areas of weakness that can cause vulnerability to threats while shifting to a remote workforce.

EMERGING SECURITY TRENDS

IDENTITY & ACCESS MANAGEMENT: Identity is a core security control that is gaining greater significance as more of today’s modern IT environments rely on identity as the main security control

Today, we will focus on three of these emerging security trends: **Cloud Computing**, **Connected Devices**, and **Ransomware**.



WHAT IS CLOUD COMPUTING?

Cloud Computing is the use of a collection of services, applications, information and infrastructure composed of pools of computer, network, information and storage resources. These components can be rapidly orchestrated, provisioned, implemented, decommissioned and scaled up or down, providing for an on-demand, utility-like model of allocation and consumption.

There are five primary service models for Cloud Computing

- **Software as a Service (SaaS):**
  Provides a full application to the organization where the service provider manages the full technology stack.

  Examples: Gmail, SalesForce

- **Platform as a Service (PaaS):**
  Similar to SaaS, but the organization manages the application layer while the service provider manages the rest of the technology stack.

  Examples: Google App Engine,
  Amazon Web Services (Beanstalk)

WHAT IS CLOUD COMPUTING?

In addition to these service models, Cloud solutions can be deployed in two different ways:

PUBLIC

Cloud environments that are managed or hosted by a service provider using shared computing resources and provided over the open internet.

PRIVATE

Cloud environments that are managed or hosted internally or externally, but the infrastructure is dedicated to one organization’s use.

Many organizations choose to adopt a hybrid of these deployment models, leveraging **private** clouds for services with a lot of sensitive data or a need to comply with regulatory requirements and **public** clouds that need to be agile, flexible, and scalable.

CLOUD COMPUTING RISKS

Adopting cloud computing has significant benefits for organizations and can enable a more nimble and scalable solution without the need to manage the details.

However, organizations should consider the following questions to identify if they are at risk for a cybersecurity event.

How are we managing user identities across cloud environments?

Adopting a cloud environment, especially a public cloud, extends the organization's security perimeter beyond the traditional on-premise environment, forcing increased reliance on tight identity control.

Are we prepared to extend our cyber risk controls to our cloud environment?

Traditional cybersecurity controls need to extend to the cloud at a time when many enterprises are barely keeping up with on-premise controls.

How are we securing our data to protect against a provider breach?

Cloud providers are a more valuable target to attackers because of the large concentration of data. Attackers, go "where the data is" for the biggest score.

Do we have a full understanding of our cloud footprint?

The ease of implementing a cloud solution can lead to shadow IT within the environment. Research shows that most organizations they have **40** cloud applications deployed, but the average number of cloud applications used per organization is over **1,200**.

CONNECTED DEVICES

Connected Devices (also called the “Internet of Things” or “IoT”) is an environment in which “things” – objects, animals or people – are given unique identifiers on the internet and are able to transfer data over a network without the need for human-to-human or human-to-computer interaction. The IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems and the internet.

DATA COLLECTION

At the core of the IoT are sensors and actuators that collect, transmit, store and act on data at the source. These devices range in size and capability. Some have minimal operating systems and others have robust embedded OSes.

CONNECTIVITY

The IoT cannot exist without the interconnection of devices and sensors. Bluetooth, near-field communication, wi-fi and cellular are familiar technologies for enabling connectivity.

PEOPLE & PROCESSES

The value proposition behind the IoT is based on the idea that action will be taken based on this data. This is where people, process and risk management come into play. Process must be designed to ensure data-driven actions are well-thought-out, consistent, and aligned with strategic objectives and risk management protocols

The real promise of connected devices lies in this third component. The integration of people and processes in the IoT is required to help the internet of everything, or IoE, evolve.

CONNECTED DEVICE RISKS

> “IoT without security = Internet of Threats.”

Stéphane Nappo
CISO, OVHcloud

Organizations that deploy Connected Devices into their environments face a variety of threats as a consumer of the technology:

- Increased Attack Surface for Cybersecurity Attacks
- Challenge Identifying and Maintaining an Inventory of Connected Devices
- Data Integrity
- Data Privacy Issues
- Device Availability/Up Time
- Compliance Risk
- Rapidly Evolving Compliance and Regulatory Environment
- Managing The Device Lifecycle

RANSOMWARE

In the past, ransomware was simply data encrypting software used to take data hostage and demand a payment from the victim. Today, ransomware attacks have evolved beyond mere malicious encryption of data. These attacks add data theft and aggressive extortion.

> **Ransomware attacks are the manifestation of an intrusion, not a unique attack or piece of software.**

HOW DO THESE ATTACKS TARGET AN ORGANIZATION?

Attackers develop techniques and an entire underground ecosystem to deliver an attack and monetize it. Simply put, ransomware attacks are a business. If your lack of defenses make it easy, they will strike. If your defenses stay static, they will innovate. If you can pay, they will return.

RANSOMWARE ATTACKS ARE EVOLVING

Attackers are getting even more bold with their ransomware and have started to focus their attacks based on new criteria.

TARGETING BACKUPS

After initial access is gained, Ransomware attackers will search the network for your backups and delete them.

DUMPING EXFILTRATED DATA

Ransomware attackers are dumping exfiltrated data (data stolen during the attack) on public sites to inflict reputation damage on the victim organization.

REPORTING BREACH

Ransomware attackers are using the threat of additional regulatory fines and penalties to increase pressure on the victim organization

LEVERAGING CYBER INSURANCE

Ransomware attackers will search for cyber insurance policy info to determine coverage levels and better tune the demands.

MARKET DEVALUATION

Ransomware attackers are looking for opportunities to leverage the ransomware attack to drive market movement around the victim organization's stock price. An example technique includes shorting the victim's stock prior to the attack.

MONETIZING STOLEN DATA

Ransomware attackers are sifting through exfiltrated data to find ways to further monetize it on the dark web.

RANSOMWARE BEST PRACTICES

> “Ransomware is more about manipulating vulnerabilities in human psychology than the adversary’s technological sophistication.”
>
> James Scott
>
> Sr. Fellow, Institute for Critical Infrastructure

The good news is that organizations can take action to prevent or lessen the impact of a ransomware attack.

UNDERSTAND RELIANCE AND IMPACT OF THIRD PARTIES

Ransomware doesn’t just need to target your organization; your third party providers can also be an attack vector. Consider how your organization could be impacted by a ransomware event at your critical third parties and implement mechanisms to reduce that dependency or minimize the impact of a third party outage.

QUANTIFYING THE IMPACT OF A RANSOMWARE EVENT

Its easy to not spend money on a hypothetical risk like ransomware. Organizations can help justify the investment by quantifying (in dollars) the potential impact of a ransomware event.

HOW CAN INTERNAL AUDIT RESPOND?

As Internal Auditors, there are several ways to respond to the evolving cybersecurity landscape. Start by asking yourself these questions:

- What cybersecurity framework(s) does the organization use?
- Do the selected framework(s) help meet our IT and cyber compliance obligations?
- Do we have sufficient IT hygiene to keep pace with the latest cyber trends?
- Have we established roadmaps & actions to meet our desired maturity?
- Have we reconciled our cybersecurity framework(s) to the IT audit universe to confirm coverage?
- How are we managing emerging cyber risks (e.g., IoT, quantum)?

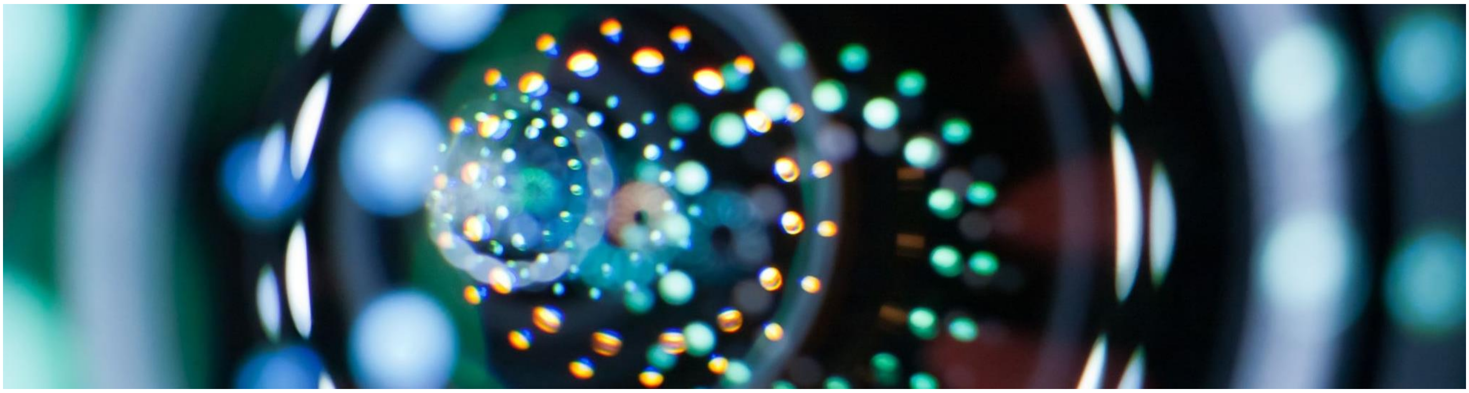
Then it is time to consider the types of assessment activities to include in the annual audit plan.

SAMPLE AUDITS

Below are several examples of audits that can provide your organization with additional insights into its cybersecurity risks:

- 3rd Party / Cyber Risk Management Program Audit
- Phishing Review
- Network Scan / Vulnerability Assessment
- Incident Response Readiness Assessment
- Security Program Maturity Assessment
- Privacy Program Review
- Identity (IAM) & Privileged (PAM) Access Management Review
- Industrial Control System (ICS) Security Audit
- Ransomware Preparedness
- IoT Program Audit
- Cloud Security Audit
- Microsoft 365 Security Assessment

+ Access example audit programs at KnowledgeLeader.com
Contact the presenter to receive a free trial.



ON THE HORIZON

Organizations cyber defenses are also evolving to respond to these increasing threats. Here are several new trends to discuss with your first line of defense:

ZERO TRUST ARCHITECTURE

How is your network evolving to reduce implicit trust between systems?

QUANTUM-RESISTANT CRYPTOGRAPHY

How will your encryption strategy hold up in a quantum world?

PASSWORDLESS AUTHENTICATION

How will your organization move beyond the password to protect systems access?

AIR-GAPPED NETWORKS

How are critical networks separated from business networks?

ABOUT THE PRESENTER

Tim Maloney is a Director in Protiviti's Technology Governance & Risk Management practice where he partners with executives to get the most value from their IT functions. In his 20 years with Protiviti, Tim has helped organizations across a variety of industries to identify and respond to their most significant IT risks. He believes that business problems are best addressed through realistic recommendations that align with his client's corporate culture and capabilities.

CONNECT WITH TIM

in	@TMaloneyJr
🐦	@TimMaloneyJr
✉	Tim.Maloney@protiviti.com
🌐	Tim-Maloney.com

Face the Future with Confidence

protiviti®