2024 State of Cyber Report

The Top 4 Challenges
Cybersecurity Leaders Face Today

BDO DIGITAL

BDO

Introduction

Cyber threats are seen as the **third most impactful risk to businesses** over the next three years, after the cost of capital and economic downturns, respectively. Threat actors are not only deploying new tactics using generative artificial intelligence (AI) to conduct more targeted and sophisticated attacks, but are also advancing familiar threats like ransomware with increased severity. The evolving regulatory landscape and the increasing adoption of cloud software also pose new challenges for cyber leaders.

> *Given the scale and prevalence of cyberattacks, it is virtually impossible to avoid and eliminate them — but that doesn't mean your business can't prepare. Not only is it important to understand and address the cyber risks that businesses face today, but you also must measure the ROI and effectiveness of your cybersecurity investments. This is essential for organizations to effectively protect their teams, data, customers, and stakeholders.*

RIC OPAL
BDO Digital Segment Leader,
Cyber & IT Solutions

Are you prepared to navigate the threat landscape this year?

Table of Contents

Challenge #1

Generative AI is Enhancing Cyberattacks

While AI has allowed enterprises to drive advanced data analysis, communication, and operational efficiency, it has also enabled threat actors to conduct more sophisticated cyberattacks. Cybercriminals now use the power of AI to achieve their ends more effectively. AI enhances existing tactics and enables new types of attacks, which is why security leaders must evolve their defenses — quickly.

Though generative AI poses new threats, it's also proving to be instrumental in supporting cybersecurity efforts. While human error accounts for over **80% of cyber incidents**, AI can help cyber leaders bridge critical gaps, automating tasks and recognizing patterns invisible to the human eye.

Challenge #1

GENERATIVE AI ENHANCES EXISTING ATTACKS

Generative AI-powered cyberattacks use machine learning (ML) to analyze human and machine targets and identify attack techniques most likely to compromise an organization. Generative AI allows threat actors to examine stolen data more quickly and on a much larger scale.

For example, instead of one-off password exploitation, attackers now use generative AI to fuel massive password-cracking schemes. Attackers also use generative AI to automate attacks, causing them to cause more damage with minimal manual intervention. Generative AI-powered bots autonomously power web scraping attacks that mimic human behavior while gathering code and data at exponential speeds.

Generative AI also aids the creation of sophisticated and highly effective malware that is more stealthy and evasive than its predecessors. Attackers use generative AI algorithms and ML to automate the malware creation processes, streamlining and speeding up their efforts. Not only are hackers leveraging generative AI platforms as a tool in their arsenal to create malware, but they are also using large language models (LLMs) to spread malicious code into target environments.

GENERATIVE AI ENABLES NEW ATTACKS

Generative AI harnesses massive amounts of human-generated text and applies ML algorithms to predict or generate new text, video, audio, and images. While extremely helpful for well-meaning people, generative AI has made social engineering easier and enables attackers to leverage even more sophisticated tactics. For example, hackers are using generative AI to produce convincing phishing emails, which are increasingly harder to catch. Notoriously telltale signs of a phishing scam, like misspellings and grammatical inaccuracies, are far less likely to occur now. Instead, generative AI tools are helping hackers overcome language barriers and create realistic, contextually relevant, and persuasive "human-like" responses intended to be malicious.

Threat actors are also using deepfakes — generative AI-generated images and videos that seem real — to hijack systems, gain access to confidential data, and fuel disinformation attacks. Ahead of the 2024 elections, an expected influx of threat actors will likely use generative AI to create and spread fake news to potentially influence the 4 billion people voting in over 40 countries this year.

Recommendations

Generative AI, when leveraged responsibly and with the appropriate governance measures in place, can provide security professionals with advanced tools to navigate cybersecurity challenges and become more agile in the face of threats. Organizations looking to improve cybersecurity and mitigate security risks benefit from generative AI in a number of ways.

1

Increasing response speed

Automating early threat detection shortens the time between attack and discovery through early warnings, speeding up responses. Generative AI can automate incident response, helping organizations contain attacks, reduce human effort, and limit damage. Attackers begin moving laterally within **1 hour and 42 minutes** on average, making each moment critical.

2

Identifying trends in data

Generative AI can effectively leverage historical data sets, like ticketing logs, data from previous attacks, industry insights, and more, to predict potential attack vectors. Predictive AI can **streamline threat detection** and put organizational data to work to protect the business.

3

Understanding the threat landscape

Technology like **Microsoft's Security Copilot** and **Sentinel** use AI to help improve risk detection. These tools analyze network changes and large data sets, using behavioral analytics and anomaly detection to identify unusual activities.

BDO Digital can help you leverage generative AI to help improve your cybersecurity strategy.

GET STARTED ▶

Challenge #2

The Ransomware Threat is Growing

Ransomware continues to plague security leaders and is poised to cost its victims **$265 billion annually** by 2031. In fact, global ransomware activity alone was **up 50%** year-over-year during the first half of 2023 and is expected to continue to grow in 2024. The loss or exposure of data causes more than just significant financial impacts — it also poses substantial reputational and operational risks and jeopardizes hard-earned customer trust.

To address cyber risk, business leaders must translate their concerns into action.

Challenge #2

RANSOMWARE TACTICS ARE EVOLVING

New tactics like double and triple extortion are of growing concern to companies and individuals alike. Today, hackers not only encrypt a victim's files but also threaten to publicly release the data unless a ransom is paid. These extortionary tactics threaten reputational damage, along with the loss of trade secrets, sensitive data including personally identifiable information (PII), and more.

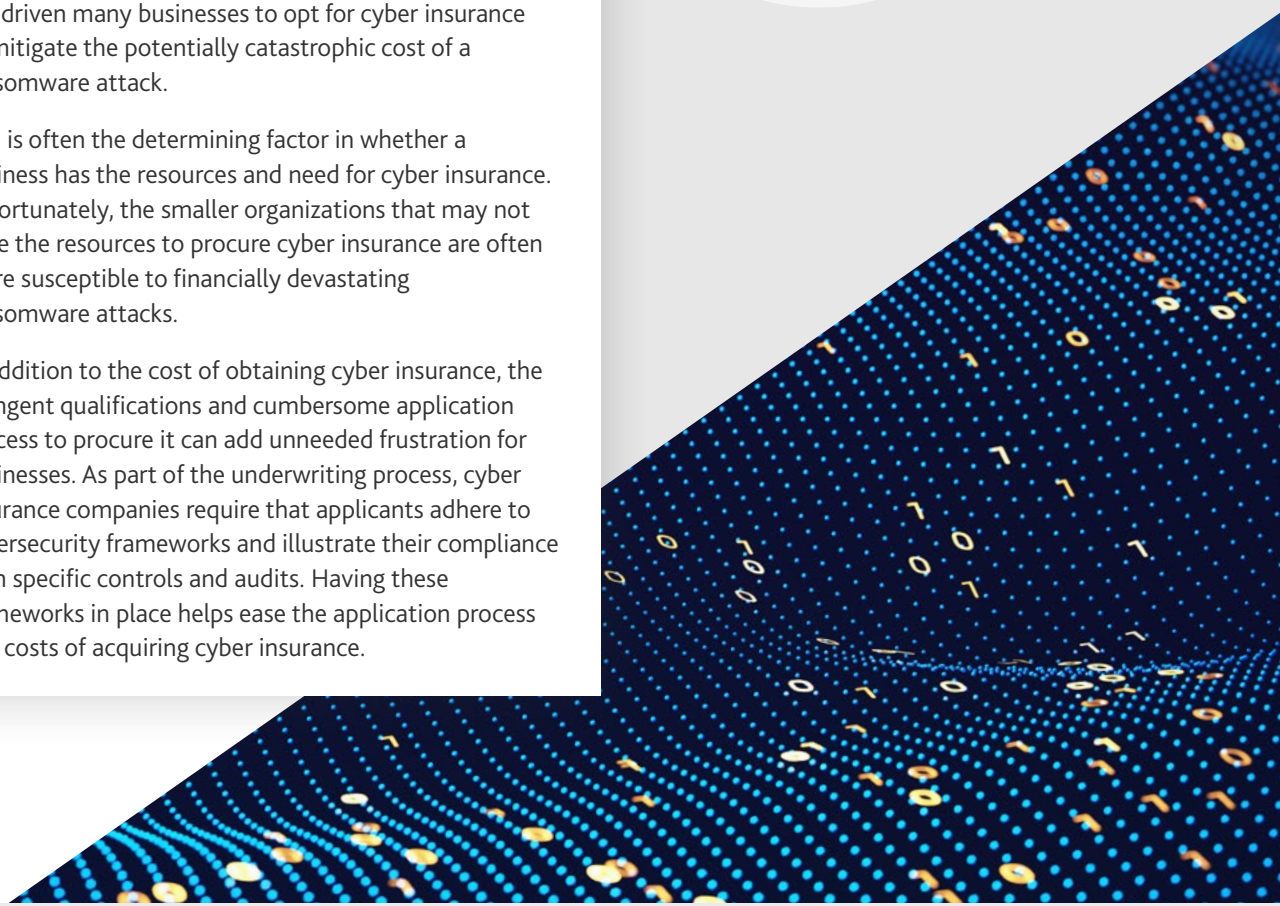
Ransomware has historically been a time-consuming, highly manual effort. Generative AI, however, has also allowed threat actors, even those with less experience, to automate and speed up their ransomware distribution efforts, increasing the potential payout for cybercriminals. Threat Actors will also use generative AI to research potential targets across social media platforms to launch a more focused attack.

THE ROLE OF CYBER INSURANCE

Organizations have the responsibility to protect their client, investor, and employee data. In addition to having an incident response (IR) plan and increasing overall cyber hygiene, the prevalence of ransomware attacks has driven many businesses to opt for cyber insurance to mitigate the potentially catastrophic cost of a ransomware attack.

Size is often the determining factor in whether a business has the resources and need for cyber insurance. Unfortunately, the smaller organizations that may not have the resources to procure cyber insurance are often more susceptible to financially devastating ransomware attacks.

In addition to the cost of obtaining cyber insurance, the stringent qualifications and cumbersome application process to procure it can add unneeded frustration for businesses. As part of the underwriting process, cyber insurance companies require that applicants adhere to cybersecurity frameworks and illustrate their compliance with specific controls and audits. Having these frameworks in place helps ease the application process and costs of acquiring cyber insurance.



Recommendations

Basic security hygiene protects against 98% of ransomware attacks, according to Microsoft. In other words, it's not to be taken lightly. The following recommendations can help improve cyber hygiene and, in turn, ransomware preparedness.

1

Create a culture of vigilance

Organizations should educate employees about the risks of social engineering tactics like phishing. Given that most breaches prey on employee error, all stakeholders need to understand their roles in preventing and mitigating the effects of a cyberattack. Leaders must not only invest in employee training but also break down the internal silos that hamper collaboration when it is most needed.

2

Plan for the worst

Unpreparedness creates risk for organizations and opportunities for threat actors. Organizations should create and/or update their IR plans to provide a proactive roadmap to follow when a threat arrives — and peace of mind in the meantime.

3

Practice, practice, practice

When it comes to ransomware attacks, experience matters. Run tabletop exercises to identify potential gaps and make sure mitigation and recovery processes are sound. Conduct point-in-time security assessments to confirm that security solutions meet the organization's needs and are relevant to its size and industry.

BDO Digital offers a range of point-in-time security assessments. To begin, request a free attack simulation.

GET STARTED ▶

Challenge #3

Maintaining Compliance in an Evolving Regulatory Landscape

New laws and regulations are continually rolling out to protect businesses, consumers, and critical industries against threats that are taking advantage of advancements in technology. Various stakeholders, including regulators, shareholders, and customers are increasingly demanding accountability and have an interest in organizations' compliance efforts.

Challenge #3

GROWING REGULATORY PRESSURE

The European Union's General Data Protection Regulation (GDPR) sets the standard for defining and setting data protection and privacy guardrails for data controllers. While not mandated, more U.S.-based organizations are adopting GDPR standards. Even those who don't embrace GDPR may, nonetheless, find that many U.S. local and state governments are pushing for stricter privacy laws. Following California's lead, new location-specific privacy rules in Florida, Oregon, and Texas are set to go into effect in July 2024. Montana and Washington will enact privacy laws later this year.

Increasing regulatory pressure in the U.S. also means companies need to disclose material incidents quicker than ever before. These regulations include new reporting requirements outlined in the Securities and Exchange Commission's (SEC) cybersecurity disclosure rules and the Federal Trade Commission's (FTC) amended Safeguards Rule. These rules also outline a company's broader risk management, strategy, governance, and oversight responsibilities.

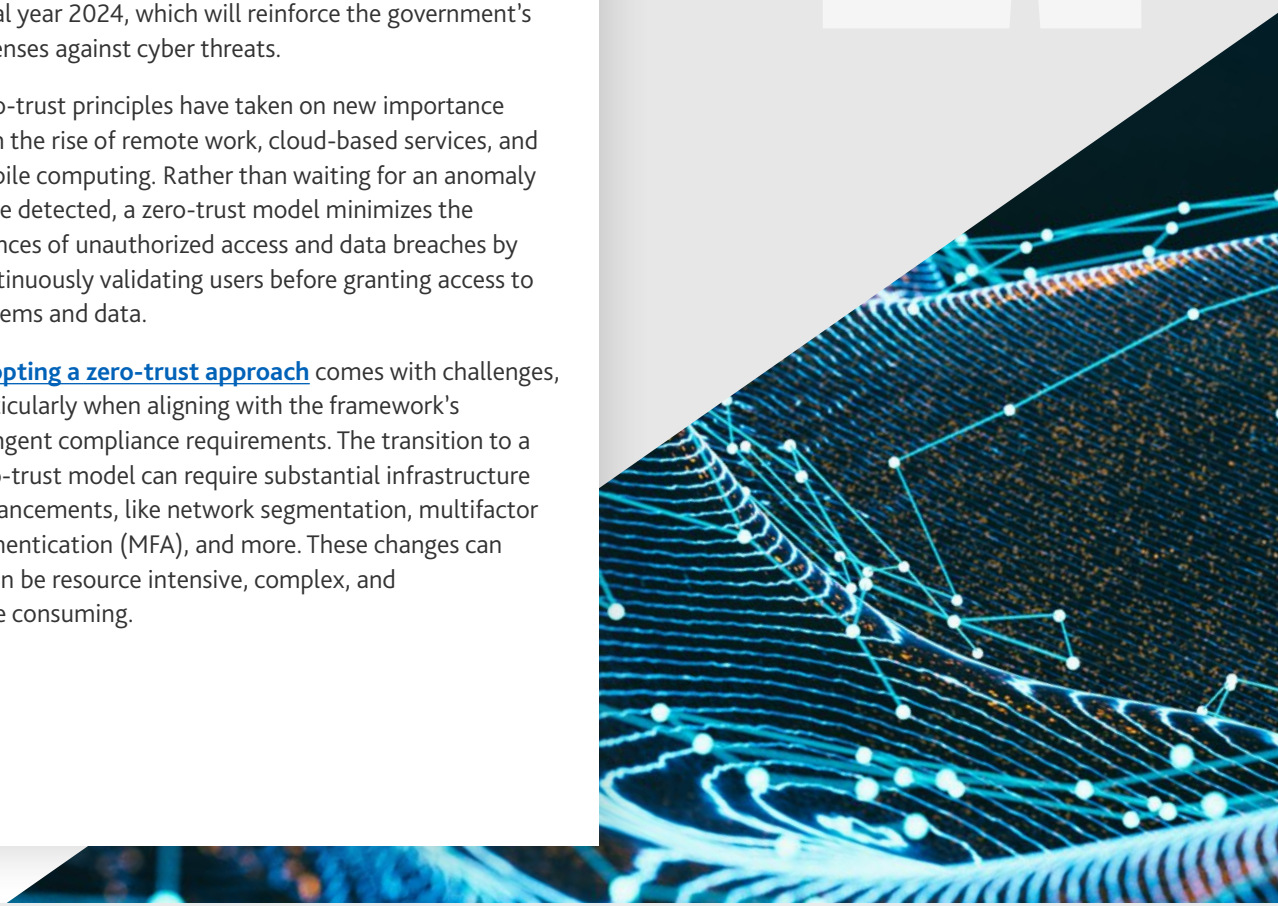
While these regulations are directed at public companies, anyone who works for or with public companies will also be impacted. Ultimately, the interconnected nature of today's business landscape means that private companies should anticipate the effects of these regulations and prepare now.

ALIGNING WITH ZERO TRUST

First issued in January 2022, the White House's zero-trust strategy mandates that all federal government agencies complete several zero-trust tasks by the end of fiscal year 2024, which will reinforce the government's defenses against cyber threats.

Zero-trust principles have taken on new importance with the rise of remote work, cloud-based services, and mobile computing. Rather than waiting for an anomaly to be detected, a zero-trust model minimizes the chances of unauthorized access and data breaches by continuously validating users before granting access to systems and data.

Adopting a zero-trust approach comes with challenges, particularly when aligning with the framework's stringent compliance requirements. The transition to a zero-trust model can require substantial infrastructure enhancements, like network segmentation, multifactor authentication (MFA), and more. These changes can often be resource intensive, complex, and time consuming.



Recommendations

A proactive approach to risk management is critical to make sure compliance is maintained at all levels. When approaching compliance, consider the following recommendations.

1

Reinforce the importance of education

To avoid the legal and reputational consequences that can stem from noncompliance, continued education is crucial. As part of a broader risk management program, train employees at all levels of your organization on cybersecurity and zero-trust policies and best practices.

2

Create a timely risk assessment process

Reassess critical systems every 18 to 24 months to identify emerging threats and keep organizational security up to date. This assessment helps establish and enforce a cybersecurity roadmap that demonstrates the organization's plan to regulatory stakeholders and partners.

3

Implement a robust system for regular compliance audits

Regular internal audits promote adherence to regulatory requirements and increase preparedness for external audits. A Security Operation Center (SOC) for Cybersecurity report may also prove valuable to gain actionable insights and third-party validation of cybersecurity preparedness.

Help enable your people, processes, and technology with BDO Digital's complementary security and compliance consultation.

GET STARTED ▶

Challenge #4

Cloud Migration Risks

Cloud computing has protected organizations at scale and has allowed them to gain efficiency. **Ninety-four percent of all companies globally use cloud software**; however, its widespread adoption poses significant security challenges. Data loss, breaches, and privacy concerns remain high as cybercriminals ramp up their efforts to infiltrate corporate networks.

Cloud account threats increased **16-fold in 2023**, impacting three times as many organizations compared to the year prior. As more systems and data move to the cloud this year, the prevalence and severity of cloud based risks will likely increase.

Challenge #4

MISCONFIGURED CLOUD STORAGE AND THE VULNERABILITIES IT PRESENTS

While the cloud promises increased mobility, collaboration, and speed, it also presents opportunities for mishandled data. Managing various vendor-specific security settings, for example, can result in misconfigurations, leaving cloud assets vulnerable to malicious activity.

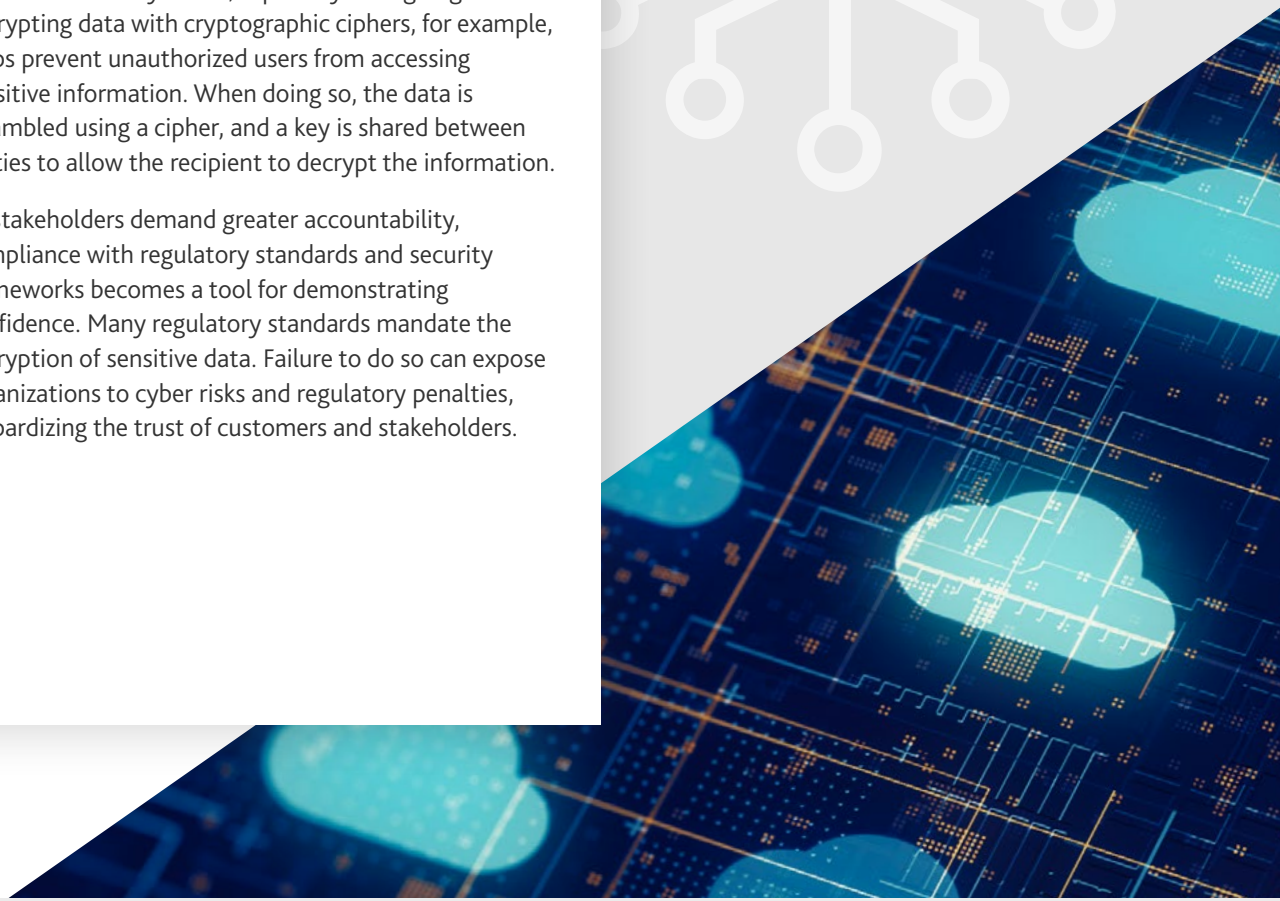
Misconfigured cloud storage can create opportunities for unauthorized access and breaches of sensitive data. Cloud providers have different default configurations with specific nuances and implementation guidance, making it difficult to secure various cloud services. Adversaries exploit these misconfigurations by gaining administrative privileges, which enables them to release corporate and personal information, introduce malware, and more.

Most enterprises have hybrid or multi-cloud deployments, which can make data difficult to monitor and data access hard to control. When multiple services need to interact, the attack surface is increased as are the inherent complications of interfacing multiple systems and platforms.

IMPORTANCE OF ENCRYPTING DATA FOR MIGRATION

Data requires protection at rest and while in transit. Encryption is the best strategy for avoiding common cloud data security issues, especially during migration. Encrypting data with cryptographic ciphers, for example, helps prevent unauthorized users from accessing sensitive information. When doing so, the data is scrambled using a cipher, and a key is shared between parties to allow the recipient to decrypt the information.

As stakeholders demand greater accountability, compliance with regulatory standards and security frameworks becomes a tool for demonstrating confidence. Many regulatory standards mandate the encryption of sensitive data. Failure to do so can expose organizations to cyber risks and regulatory penalties, jeopardizing the trust of customers and stakeholders.



Recommendations

Spending on public cloud services is forecast to grow by **more than 20%** this year, according to Gartner. This growth is likely driven by an increase of the usage of cloud for advanced technologies such as generative AI, ML, Internet of Things (IoT), and other applicable use cases. As use cases evolve, so too do the risks. To prepare for cloud migrations, consider the following recommendations.

1

Implement a zero-trust policy

Control who has access to sensitive cloud data to limit the possibility of data breaches. With a zero-trust policy, a business can grant minimum data access to employees and keep highly sensitive data out of reach. Role-based access gives employees role-specific data permissions based on their job responsibilities.

2

Leverage a comprehensive monitoring solution

Following a migration, use a monitoring solution to screen the threat landscape while identifying and closing loose ends. Establish regular data backup schedules along with real-time monitoring and detection systems to reduce the risk of data loss, increase transparency, and proactively alert teams when a potential security incident arises.

3

Create a thorough cloud-centric IR plan

A well-defined, cloud-specific IR plan helps maintain data availability and business continuity during and after a migration. Put a plan in place ahead of migration to help response teams navigate any unforeseen issues or data loss scenarios.

BDO Digital offers robust cloud services to keep your data safe on your digital transformation journey.

GET STARTED ▶

Looking Forward

While organizations concentrate on protecting their systems, people, and stakeholders, the sheer scale and frequency of cyberattacks can make it nearly impossible to entirely prevent them. However, businesses can still cultivate long-term resilience if they are dedicated and prepared to doing so. Developing cyber resilience is crucial for organizations to be ready for, respond to, and recover from cyberattacks.

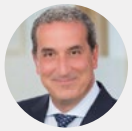
Connect with our team now to discuss your 2024 cyber strategy and how to navigate the cyber challenges facing your business.

Handling cyber incidents appropriately is crucial for building trust, maintaining compliance, and keeping your business running smoothly. At BDO Digital, we believe cyber resilience extends beyond security controls; it's about creating a culture of security rooted in a deep understanding of the evolving risk landscape. That means prioritizing risk management, incident response, and continuous improvement while continually evaluating your threat profile as your business evolves.

ROCCO GALLETTO
BDO Digital Principal,
National Cybersecurity Leader

CONTACT US

RIC OPAL
BDO Digital Segement Leader,
Cyber & IT Solutions
630-686-4302 / ropal@bdo.com



ROCCO GALLETTO
BDO Digital Principal,
National Cybersecurity Leader
289-266-1403 / rgalletto@bdo.ca

BRAD ELLISON
BDO Digital Market Leader,
Cyber & IT Solutions
630-286-8196 / bellison@bdo.com

BDO Digital, LLC is a Delaware limited liability company, and a wholly-owned subsidiary of BDO USA, P.C.

BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information on BDO Digital, LLC please visit: www.bdodigital.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2024 BDO USA, P.C. All rights reserved. www.bdo.com