Insight

The CISO's Guide to Overcoming Cybersecurity Challenges

Lead your organization to a new, safer vantage point.

Security is a Herculean task.

As security teams resolve one risk, it's common for several more to appear. And every challenge is connected. Between alert fatigue, disparate tools and the never-ending, always-changing nature of the beast, staying on top of it all — much less getting ahead — seems close to impossible.

At Insight, our security work across every industry has revealed three main categories where cybersecurity poses real challenges, and opportunities, to elevate your program:

Evolving cyberthreats

Cost and complexity

Regulation and compliance

Read on to learn what it takes to conquer these summits and how new strategies can prime you for innovation in a rapidly changing threatscape.

FOCUS AREA #1:

Evolving cyberthreats

From email inboxes to the national news, you don't need to look far to know that the problem of ransomware has been spiraling out of control. And with ransomware tactics evolving rapidly, it's even harder to rein in the problem.

The birds-eye view can be overwhelming: rapidly evolving dispersed infrastructures, increasingly sophisticated attackers and an abundance of valuable data just waiting to be looted and leveraged for criminal gain. What's more, there is an abundance of security solutions that still don't seem to be doing the trick.

82% of security leaders have been surprised by a security event, incident, or breach, which evaded a control they thought was in place.[1]

In an era of "when, not if," cyberthreats are difficult to pinpoint and fend off because organizations simply can't predict them. This is why a multilayered approach encompassing risk mitigation and risk minimization has become more critical than ever.

4 Best Practices for Ransomware Readiness

The top industries targeted by ransomware are technology, healthcare and education[3] — but all are at risk. No matter your market, these best practices will help you ward off attacks and respond more effectively to incidents:

1. Know your vulnerabilities.
2. Secure your data.
3. Back up your backups.
4. Have a plan.

Read this ebook for more on evolving ransomware trends and steps for strategizing your approach to security. →

Does Your Security Program Have All Your Bases Covered?

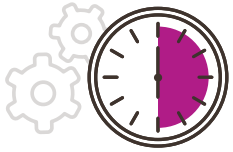
Security should help you save costs and streamline operations. Watch this video from Insight security experts to learn how risk-savvy organizations can create and implement a comprehensive approach to security as part of business transformation.

Watch now →

FOCUS AREA #2:

Cost and complexity

Your organization could have 76 security tools in place (the average number in a given organization[1]) and still leave your business wide open to risk. Operating with disjointed legacy solutions and an abundance of new tools creates overlap, overwork, blind spots and silos.



Security teams
spend more than half of their time
manually producing reports.[1]

This type of security environment creates more vulnerabilities and is also a drain on resources. And yet, this is where many organizations operate — in a multi-vendor security space resulting in overwhelm, overspending and underperformance.

The core issue behind this cost and complexity? Lack of strategic expertise. Investing in defensive tech without informed, strategic and technical guidance for adoption, deployment and integration is a recipe for disaster:

- Gaps between tool sets
- Lack of data integration
- Mounting technical debt
- Overburdened teams
- Reduced risk resilience

FOCUS AREA #3:

Regulation and compliance risk

Security runs the gamut from the granular to the giant: from personnel passwords to data protection strategy. All of it has the potential to impact your regulatory and compliance risk.

Understanding your risk

Regulatory risk

Regulatory risk is your vulnerability to changes in regulations or legislations set by the governing bodies that oversee your industry. The impacts of a regulatory change can introduce increased costs, administrative challenges, legal concerns, and have the potential to slow or halt business.

Compliance risk

Compliance risk is your exposure to legal penalties and financial and reputation loss due to failure to comply with industry laws, internal policies and best practices. Companies handling sensitive information face increased risk in the area of data privacy — noncompliance can result in devastating business consequences.

The complexity of today's business processes means there's no simple, foolproof method for mitigating risk. It requires communication and strategy across executive, operational and technical teams to create full visibility and awareness.

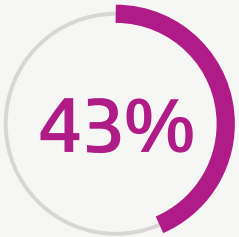
Questions for guiding regulatory and compliance risk management include the following:

- Are established protocols in place for regularly assessing regulation and compliance?
- Are you currently meeting government, market and industry regulatory requirements?
- How aware are you of the potential losses or risks if found noncompliant?
- How quickly would you be able to respond to a regulatory change?
- How does your organization perform under audits?
- Is IT involved in compliance risk management?

Security success stories we love

In the wake of a TSA security directive and a high-profile outage, this natural gas utility company conquered a complex task list to meet aggressive timelines with unmatched speed and accuracy.

Read the full client story **to see how we worked together to consolidate workstreams and execute.** →



of security professionals **have little to no understanding of best practice measures, metrics and policies** used by peer organizations.[1]

say a **lack of a unified, proactive approach to security and governance** is inhibiting progress with innovation[2]

5 traits of a winning cybersecurity strategy

Arming the full spectrum of your IT environment — from core to edge — is key.

The Insight-commissioned 2022 IDG report on digital transformation, "The Path to Digital Transformation: Where IT Leaders Stand in 2022," found that

36% of respondents say mitigating risk with stronger cybersecurity programs is a top objective.[2]

Our goal is to help you get there.

In the process of crafting a stronger cybersecurity strategy, everything matters, from how you choose and implement infrastructures to the protocols you put in place to protect them.

Consider this next section your guide to approaching the cybersecurity fight with both offensive and defensive strategies.

We'll cover the top solutions and protocols we see our clients using to successfully protect and defend their organizations.

1.

Adopt a Zero Trust framework.

Remote connectivity directly expands the network perimeter, and where the network perimeter goes, security risk follows. The very nature of today's model for connectivity makes it difficult to secure.

0100
1101
0010

Data is everywhere.

The network perimeter isn't fixed.

Attacks come from without and within.

This kind of sprawl makes it much harder to maintain compliance, consistently pass audits, and plan and prove an ironclad security strategy.

A Zero Trust framework provides a methodical approach to addressing and mitigating this inherent risk, protecting networks, users and data with multilayered safeguards. **There are three essential components to a Zero Trust approach:**

Workforce:
Enterprise users and devices that access enterprise applications

- Verifying user identities with Multi-Factor Authentication (MFA)
- Gaining device visibility and establishing trust
- Enforcing access policies with adaptive access controls

Workloads:
Enterprise applications, services and microservices

- Gaining visibility across your environment
- Identifying individual workloads
- Programming and enforcing policies
- Containing breaches
- Maintaining compliance
- Continuously monitoring activity
- Automatically responding to compromises

Workplace:
Enterprise endpoints and IoT devices

- Granting the appropriate level of network access to users and devices with network authentication and authorization
- Classifying and segmenting users, devices and applications
- Containing infected endpoints
- Revoking network access as needed

The goal of embedding security into the network to connect and protect all users and applications, whether on-premises or in the cloud, is possible with experienced partners for execution. And the results are powerful: **With fully integrated security, teams are freer to focus on innovation over risk management.**

Top security initiatives include:

- **68%** Performing security testing
- **65%** Implementing Zero Trust policies
- **64%** Updating governance policies
- **63%** Implementing a Security Operations Center (SOC)
  More progressive organizations are further along in SOC implementation.[2]

2.

Invest in network and edge security.

Today, most conversations around the network inevitably lead to the topic of the edge. The edge is essentially the perimieter — but in the age of hybrid work, the network perimeter is more often than not undefined, leaving most organizations open to risks.

The modern network edge

Components:

- Traditional networks
- Cloud networking
- Wi-Fi connectivity
- 5G
- VPNs

Characteristics:

- Automation
- Security integration
- Next-level service capabilities

Transform network security.

Read the whitepaper "Transforming Network Security: How to Win Against Cyberthreats" for approaches on achieving stronger network security — for the near and long term.

Read the whitepaper →

You may have heard of the "intelligent edge" — Internet of Things (IoT) devices with compute leveraged for advanced network functionality at the edge. **Key challenges facing an effective network edge include:**

- Requirement complexity
- End-of-support technology
- Lack of visibility
- Security at scale

As more users adopt hybrid and multicloud strategies, cloud-centric network security has taken center stage. Some of the strongest strategies for securing the modern network edge include Secure Access Service Edge (SASE) and SD-WAN — two solutions that use the cloud to connect and secure geographically disparate endpoints in a flexible, adaptable way.

SD-WAN

- Cloud-based network technology designed to provide increased bandwidth at lower costs, enhanced security and other benefits
- Focuses on connecting remote locations back to a central private network to control network traffic securely and efficiently
- Optimizes Software as a Service (SaaS) performance using on-ramp capabilities
- Leverages service chaining for dynamic traffic steering and application-aware routing within the enterprise

SASE

- A concept that defines the convergence of networking and security services within a cloud-based architecture
- Builds in familiar security architectures and capabilities
- Focuses on converging network and security into a unified, cloud-delivered service model
- Establishes a virtual network overlay with distributed Points of Presence (PoPs)
- Runs multiple policy engines in parallel at each PoP to inspect and secure traffic

3.

Take cloud security seriously.

Too often, organizations assume the cloud is automatically secure. It's easier to suppose cloud providers are responsible for protecting data than to take on the responsibility of adding cloud security and compliance to an already-full task list. **And yet, cloud security is a top concern:**

93%

of IT security professionals **worry that human error could accidentally expose data in a public cloud.**

37%

say that risk management capabilities in the cloud are **at least somewhat worse than in other parts of the organization's infrastructure.**

ONLY 22%

say their organization maintains continuous compliance with cloud security regulations and standards.[4]

Understanding who's responsible for data security in the cloud is only part of the challenge.
A comprehensive cloud security strategy includes:

- Cloud governance that establishes clear policies and protocols, reducing vulnerabilities
- Identity and Access Management (IAM) strategies spanning cloud and other environments
- Protection and retention strategies for data residing in or traveling to and from the cloud
- Cloud-first security postures and frameworks
- Authentication and encryption capabilities

The What, Why, and How of Cloud Security

What's driving the need for cloud security? In this video, explore pain points from visibility to control and fragmented platforms — and how businesses are simplifying, unifying and mitigating risk in large cloud and multicloud environments.

Watch now →

4.

Modernize data protection and data security.

Consider security from the standpoint of data protection. Cybercrime isn't your only threat. Data can be compromised, corrupted or lost anytime your organization pursues data infrastructure changes. **This could happen in several ways:**

- Data center and cloud migrations or consolidations
- Intentional or unintentional unauthorized user access
- Poorly managed configurations

Safeguarding data, wherever it lives, requires a deep understanding of the data you're protecting — making data discovery and classification critical. This process often starts with a comprehensive data discovery exercise, followed by defining high-level data categories. Different types of data will receive different treatments, and your overall strategy will be defined by your business's unique goals and risks.

Key points of consideration for developing a strong data protection and security strategy:

- Data lifecycle management
- Data risk management
- Data storage management
- Regulations and standards compliance
- Data soveriengty
- Data access management control
- Testing, exercising and reporting
- Continuous improvement

8 common traits of successful data protection strategies

1. A security team mindset shift
2. Tape for air-gapped backups
3. All-flash storage
4. Immutable storage
5. Two-factor authentication
6. Strong data discovery and classification processes
7. At-scale test restores
8. Ongoing efforts around data protection

Learn more in the ebook An IT Leader's Guide to Data Protection for the New Threatscape. →

5.

Make the most of Microsoft security.

Microsoft has proven to be a powerhouse for the modern workforce with products that enable collaboration and flexibility while built-in security and support protects users and devices.

Windows Security

Microsoft's Windows® devices include Windows Security built in to protect your devices from malicious software attacks.

Microsoft 365 Security

Microsoft 365™ Security is a modern cloud security solution that helps organizations streamline security operations, remove redundancies and save on costs.

Microsoft Sentinel

Sentinel is a cloud-native and scalable Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platform for visibility and analytics.

Simplify with Microsoft Sentinel.

Streamline your multi-vendor security environment with Microsoft Sentinel™. Sentinel pulls data sources from your entire ecosystem, giving your teams visibility and control to simplify threat hunting, reduce alert fatigue and capture a true picture of your security posture.

Read the ebook to learn how to implement and make the most of Microsoft® Sentinel. →

Reclaim the path to innovation.

Break free from cybersecurity complexity. Insight can help.

It's clear we're facing new challenges in cybersecurity. New challenges invites new solutions — but solutions without expert execution can add to those challenges.

While we've provided a list of practical solutions that will be crucial on your security journey, your next move is critical — working with an experienced partner in cybersecurity strategy. We'll help you identify your top challenges, execute with precision and build an approach to security that propels your organization toward innovation.

Learn more. Visit solutions.insight.com

Insight®

Sources:
[1] Panaseer 2022 Security Leaders Peer Report.
[2] Marketpulse Research by IDG Research Services. (January 2022). The Path to Digital Transformation: Where IT Leaders Stand in 2022. Commissioned by Insight.
[3] Gruber, D. and Lundell, B. (February 2020). Ransomware Still Rampant, Fueled by Insurance Companies. Enterprise Strategy Group.
[4] Lapena, R. (2020, Aug. 12). Survey: 76% of IT Pros Say It's Difficult to Maintain Security Configs in the Cloud. Tripwire.

©2022, Insight Direct USA, Inc. All rights reserved. All other trademarks are the property of their respective owners.