A CISO GLOBAL WHITE PAPER

EMA Report “Using Compliance Budget to Advance Security Priorities” Summary

Author: **Baan Alsinawi**

Table of Contents

Introduction:

Those with years of experience in the cybersecurity and risk management fields are all too familiar with the internal struggle for budget and resources waged by information technology, information security, and compliance teams. The tension is understandable. IT and information security staff are usually tasked with keeping their organizations safe from a wide range of cyberattacks, but preventive measures can be a hard sell — it can be tough to prove a tool or software solution helped the organization avoid a costly attack. Compliance teams wield regulatory frameworks and audit checklists and press the IT and information security teams to prove their efforts comply with industry security requirements. Then they report any deficiencies to management, often setting up a “We versus Them” dynamic.

But a remarkable shift is in play. A recent Enterprise Management Associates (EMA) research report, “Using Compliance Budget to Advance Security Priorities,” shows that these teams’ priorities are increasingly complementary and synchronized. And it confirms what is already being seen in the marketplace. When IT, security, and compliance teams work together to focus on real threats and ensure that their organization adheres to security best practices, the entire enterprise benefits. Security budgets stretch to cover more crucial areas, and hard-to-find resources can get more done. Even more importantly, organizations are able to strengthen and harden their security defenses.

75%

believe a **DATA PRIVACY PROGRAM** would be a **COMPETITIVE DIFFERENTIATOR**[1]

Businesses are expected to be victimized by ransomware attacks every 11 seconds, reaching every two seconds by 2031, according to research performed by Cybersecurity Ventures, and global cybercrime costs are predicted to be as high as $10.5 trillion USD by 2025. These costs include data damage, destruction, and theft; stolen intellectual property; disruptions to normal business operations and lost productivity; restoring and deleting the hacked systems; and damages to business reputations and lost business due to lack of customer trust.

The EMA report takes these macro statistics down to a micro level. It includes input and feedback from more than 200 tech and business leaders from across 10 industries and shows that C-suite executives and company managers are turning to their information security and IT teams for answers on how they are protecting their organizations. Given the very real threat of “not if, but when” these organizations and their leaders might be the next cybercrime victims, this trend would seem logical. However, until now, responses have often not aligned with rates of attack, so the shift can be seen as a significant milestone.

Organization leaders are also recognizing that they must meet industry-dictated regulatory compliance requirements, so their IT compliance/audit teams are tasked with making sure their organizations are following the regulatory frameworks and controls that demonstrate they are implementing security and technology best practices.

The report examines how compliance-related priorities have shifted the majority of respondents’ overall security strategies. Reflecting on this change, the following three themes run throughout the survey:

- Alignment of security and compliance is a good thing – for everyone.
- Leaders need to overcome attitudinal barriers to address ever-changing threats and regulations.
- Technology spending is increasing, but it is complicated.

Datapoint 1: Alignment of security and compliance is a good thing – for everyone

59%

indicated **DATA PRIVACY REGULATIONS** impacted their approach to **SECURITY**[1]

Analysis 1: Businesses are increasingly required to spend on compliance due to regulatory demands, and they will use that budget to further their risk management/security implementations. As a result, it is far better that security and compliance go hand-in-hand and are complementary rather than competing priorities. The survey showed that 89% of the respondents said their information security and IT compliance priorities were generally aligned. And it's a good thing — because more than 93% indicated that compliance has shifted their security strategy, and almost 20% had completely changed their security strategy to address compliance needs. More than 80% responded that their organization's overall information security posture had increased in complexity in the past two years.

Respondents had the same top two challenges for information security and audit/compliance: data security/privacy regulations and multiple IT environments. Data security was also the top spending priority, with more than half saying they make a significant investment in data security/privacy management and data loss prevention. This trend should continue, especially as Congress considers privacy legislation that could make industry-specific compliance regulations requirements for all organizations, regardless of sector.

75%

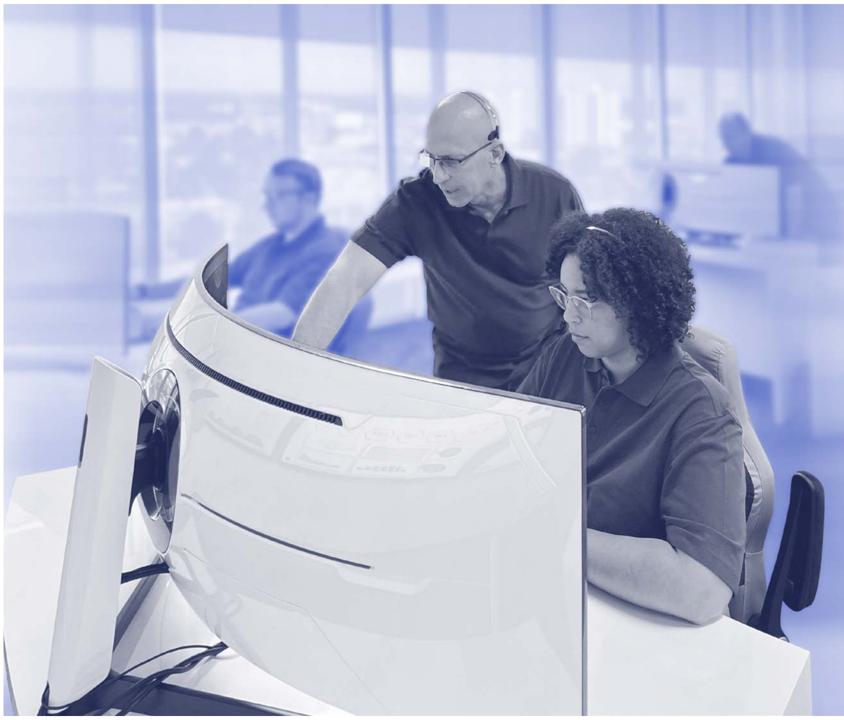
indicated **DATA PRIVACY REGULATIONS** impacted their approach to **SECURITY**[1]

The majority of respondents also said their internal IT teams provided both information security and audit/compliance functions, reducing the "us/them" mentality. Additionally, almost 90% said that their security teams worked with other technical teams for problem resolution. As compliance goals are usually aligned with an organization's business priorities, it makes sense that the information security strategies have shifted to meet these business goals. Thus, information security projects and goals are starting to be selected based on these specific business needs.

The reality is, compliance is the reason and the driver for most businesses to pay attention to their cybersecurity. Compliance is the tail that wags the dog. Businesses will choose to ignore their cyber hygiene and best practices in favor of protecting their bottom line until compliance becomes a must-do, then the calculation changes. Using compliance as a "stick" works every time. If compliance standards had more teeth, this would make a huge change in the cyber posture overall, forcing businesses to stop treating their cybersecurity requirements as an afterthought.

Datapoint 2: Leaders need to overcome attitudinal barriers to address ever-changing threats and regulations

Analysis 2: A significant percentage of respondents said they needed to improve their organization's cybersecurity culture and understanding of cyber impacts; felt the need



for a unified cybersecurity strategy across their organization; and had organizational silos, with a lack of interorganizational cooperation and shared resources. They also indicated that they lacked executive management buy-in and support, faced internal roadblocks for cybersecurity initiatives, or did not have an executive voice dedicated to cybersecurity. Organizations cited challenges dealing with different compliance obligations that constantly changed, so they were sometimes forced to deal with conflicting standards and requirements.

Having more skilled cybersecurity resources was second in how respondents felt their organizations could improve their cybersecurity, and the lack of skilled staff ranked fourth in what respondents listed as their organization's greatest security problem/challenges. Though faced with this lack of skilled resources, only around 9% used third-party cybersecurity contractors or managed service providers.

The bottom line is, organizations that have solid compliance resources should hold onto them for dear life.

Datapoint 3: Technology spending is increasing, but it is complicated

Analysis 3: The Chief Information Officer/ VP of Information Technology was by far the ultimate decision-maker in terms of who owned the budget for both information security and compliance. Correspondingly, the IT department owned the majority of the budget, with the information security department a close second. In general, the information security department set overall security/ compliance priorities.

75%

indicated an **INCREASE** in spending **OVER** previous years[1]

The majority of respondents annually spent between $50,000 and $500,000 on IT, information security, and audit/compliance, with those spending between $500,001 and $5,000,000 close behind. Around 75% indicated an increase in spending over previous years. Respondents said they spent the most on data security/privacy tools and solutions, though spending on compliance management tools and solutions was also significant. Given respondents' stated need for more resources, around 40% indicated they were willing to make a significant investment in risk management solutions/services. However, respondents also indicated they investigated a variety of other tools and solutions, which shows that there were several competing interests for budget dollars.

40%

are willing to make a **SIGNIFICANT INVESTMENT** in **RISK MANAGEMENT**[1]

The financial computation should always be: *How much does it cost to recover from an incident?* In some cases, a company's reputation will take years and even a brand name change to recover, and even then, some never do bounce back.

Closing

The EMA survey has a lot of good news.

Corporate leaders are serious about keeping their organizations safe from cybercrime threats and attacks and are showing this commitment through increased spending on information security and compliance tools and solutions. Further, that 89% of the respondents said their information security and IT compliance priorities were generally aligned shows IT leaders are cooperating, not competing, for organizational support. This will go a long way toward reducing their organization's cyber risk and significantly strengthening its security posture.

That said, the other side of the coin still indicates some not great news.

Though respondents indicated that their organizations' overall information security posture had increased in complexity, they also reported the need to improve their organizations' cybersecurity culture and understanding of cyber impacts as well as the need to have a unified cybersecurity strategy across their organizations. Though most organizations utilize internal staff to monitor their cybersecurity vulnerabilities, implement security protections and compliance-required best practices, and prevent present and future ransomware attacks and hacks, they lack skilled staff to adequately handle the workload. On the other hand, around 40% indicated they were willing to make a significant investment in risk management solutions/services.

The key takeaways are clear:

- Always include a budget line item for your compliance management.
- Use accredited solutions and certified professionals.
- Implement continuous monitoring.

When it comes to effective cybersecurity, this is truly a case where an ounce of prevention is worth a pound of cure.

References

1. Enterprise Management Associates (EMA) research report: Using Compliance Budget to Advance Security Priorities

About CISO Global

CISO
GLOBAL

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.

STRATEGY & RISK

- Gap Analysis
- Audit/Assessment
- Third-Party Risk Management
- FedRAMP
- StateRAMP
- CMMC
- Advisory
- Virtual CISO
- Managed Compliance
- Managed GRC

CYBER DEFENSE OPERATIONS

- Extended Detection & Response
- Managed Detection & Response
- SIEM as a Service
- Threat Hunting
- Cyber Threat Intelligence
- Digital Forensics
- Vulnerability Management Program
- Attack Surface Reduction
- Cyber Incident Response

CISO

SECURITY ARCHITECTURE & ENGINEERING SOLUTIONS

- Secured Managed Services
- Advanced Firewall Management
- Identity & Access Management
- Cloud Security
- Data Protection
- Remediation

READINESS & RESILIENCY

- Penetration Testing
- Tabletop Exercises with Incident Response Retainer
- Training Programs

For more information, please contact us
480-389-3444 or visit www.ciso.inc

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
SOC 2® Type II Audited