

Confronting Cyber Compliance from the C-Suite

Insights from Omega Systems & Cavelo

Let's not mince words. Compliance is a headache.

Often a cumbersome, inefficient, reactive exercise that — to regulators, investors, advisory boards and other stakeholders — doesn't exactly instill confidence. Particularly given the rate at which cyber threats are evolving and standards are increasing, keeping pace is a considerable challenge.

CFOs, COOs and other executives, historically removed from the technology process, are now critical players in the IT arena, not only responsible for budget oversight but staring down growing compliance requirements that demand more of their time and attention in an environment riddled with challenges (e.g. new cyber threats, labor shortages, rising inflation costs, supply chain disruptions, investor pressure, etc.).

As regulators turn their attention to new industries and set substantial expectations for cybersecurity safeguards, the C-suite can ill-afford to stay idle. But simply getting involved is not enough to guarantee success. By quantifying risk and aligning your security priorities to direct and specific financial implications, CFOs and COOs can drive IT compliance and execute an organizational approach to risk management consequential to business performance and success.

Inside This Whitepaper:

The Landscape

- Proven Security Threats
- Emerging Threats

The Reality

- The Technology Reality
- The Financial Reality

The Plan

- Data Discovery & Classification
- Proactive Cyber Risk Management
- How to Infuse Compliance & Risk Management into Your Financial & Operational Strategy

Final Thoughts

The Landscape

For C-suite executives to design and deliver an effective IT compliance roadmap, they must first understand the current threat landscape – as well as recognize and prepare for its constant evolution.

Traditional data protection used to focus on a business's perimeter and the assets (hardware and software) that operated within its "walls". Yet today's borderless workplaces mean the perimeter no longer exists and instead creates an almost limitless attack surface.

To that end, while modern hackers still rely on many trusted methods to penetrate corporate networks, particularly via email, they're also increasingly employing more sophisticated attacks to disrupt operations.

Proven Security Threats

Iterations of business email compromise (BEC) remain among today's most popular cybersecurity threats if for no other reason than, well, they work. The long-heralded 'employees are your weakest link' adage remains incredibly accurate and allows hackers the simplest and most effective access point to your network.

- **Phishing/Spear-Phishing:** Via email, text or even voice call, these social engineering attacks rely on the end users' lack of attention, awareness or aptitude
- **CEO Fraud:** Targeted phishing schemes that impersonate CEOs and other executives to induce security missteps
- **Brand Impersonation:** Growing in popularity, these attacks impersonate and mimic well-known companies (e.g. Google, Microsoft, LinkedIn, etc.) and take advantage of brand familiarity

\$2.4 Billion

35% of all cybercrime losses were attributed to BEC attacks, and in 2022 the percentage will eclipse that number.


BEC has accounted for US\$2.4 billion in adjusted losses for businesses and consumers.

– FBI's 2021 Internet Crime Report

Emerging Threats

Despite plenty of success utilizing these threats, some hackers have evolved their strategies to provoke more disruptive outcomes.

Traditional ransomware threats, wherein a hacker steals sensitive data and refuses to return it without financial incentive, are seeing less success, as more and more businesses refuse to pay the ransoms and rely on data backup systems and cyber liability insurance to revert to normal operations. Seemingly unhappy with this evolution, hackers are more frequently threatening to release stolen data publicly if ransoms aren't paid, which puts C-level executives in a precarious position. In cases like these, businesses are looking at significant harm to client/investor relationships and overall reputations if and when confidential data is released.



“Distributed workforces and a greater reliance on connected devices and cloud services mean that sensitive data is everywhere. Without visibility, data becomes more vulnerable to attack. Add data sprawl to the mix and suddenly businesses are facing a challenge that traditional security technology wasn't designed to fix.”

— James Mignacca, CEO, Cavelo

The Reality

Before financial and operational executives gather their IT teams and/or MSP and MSSP resources for strategy sessions, let's consider a few realities that may be critically impacting your organization's security and compliance effectiveness — whether you realize it or not.

Whether your organization has 20 endpoints or 20,000, you'll need to better understand the key complexities inherent in both the technology and financial realms that will impact how your organization answers the below questions — and how well you achieve effective cybersecurity compliance overall.

Ask Yourself:

Does your team struggle to articulate your risk management strategy to your board of directors, in investor due diligence questionnaires or cyber liability documentation?

Do you struggle to quantify the potential financial impact to your business in the event of a cybersecurity incident?

If a breach were to occur, could you confidently demonstrate that your risk would be minimal, and your company's brand and reputation would be unharmed?

The Technology Reality

The technology world never stands still, and both business and IT leaders should consider the common hurdles and complexities contributing to failed or inefficient governance, risk and compliance (GRC) programs.

The Limitless Attack Surface

With the drastic increase in remote users, endpoints, and cloud applications, knowing where data resides is increasingly challenging. IT and security teams use a combination of processes and technologies to track digital assets (including hardware, software, cloud and sensitive data), and understand their business's internal and external attack surface. However, legacy and disparate technologies can create data silos that limit visibility to the sensitive data a business has.

The Never-ending Talent Search

As if protecting more endpoints against more unique threats wasn't enough of a challenge on its own, today's enterprises are also attempting to do so with a crippling lack of IT talent. The labor shortage has left businesses with fewer resources to ward off threats and meet the growing demands for regulatory compliance – a concerning prospect for the C-suite.

The Third-Party Risk Management Problem

Then there's the increasing complexities associated with vendor risk management. The accessibility, efficiency and flexibility that cloud applications and outsourced services provide introduces further risk to an organization's risk management and requires that businesses complete thorough due diligence and employ ongoing evaluations to ensure critical data and systems remain safeguarded when accessed or managed by third parties.

"Strangely enough, the C-suites of small businesses and global enterprises make a lot of the same mistakes when it comes to cybersecurity, not the least of which is often abdicating responsibility for the company's security posture. There's a lot of pointing fingers – at the IT department, at the outsourced MSSP, at anyone but themselves. But when regulators come calling, the buck stops at the boardroom."

*– Rick Mutzel, Security & Compliance Officer,
Omega Systems*



The Financial Reality

Of course, if you're sitting in a corner office or an executive boardroom, one significant question has been looming thus far: without writing a blank check, how can I possibly understand what's required to safeguard our assets and achieve effective IT compliance?

IBM's *Cost of a Data Breach Report 2022* indicates the average global cost associated with a security breach rose 12.7 percent year-over-year to reach \$4.35 million. That cost is even higher in certain highly targeted industries, such as healthcare and financial services.

The financial implications of cybersecurity incidents are likely to continue rising. With each incident, so increase the costs for:

- **Risk remediation** — as firms scramble to implement proactive security monitoring solutions, engage MSSPs to assess vulnerabilities and continue the hunt for skilled IT talent to manage in-house and third-party security processes;
- **Insurance premiums** — as brokers look for ways to offset the surge of activity associated with cybersecurity incidents; and
- **Non-compliance penalties and fines** — as regulators at state, federal and industry levels increase expectations and look for ways to safeguard against a rapidly transforming and dangerous threat landscape.

In order for the C-suite to achieve transparency into the true cost of a breach at their organization, they must strive to quantify the unique risks and vulnerabilities inherent in their existing cybersecurity program. Fortunately, that process is attainable.

The financial costs associated with a breach are ultimately determined by the value of the data accessed or stolen. If executives can first locate all of the so-called sensitive or confidential data across their endpoints (servers, devices, cloud applications, etc.) and organize them in a manner that applies direct value to their importance, suddenly a roadmap for cybersecurity risk mitigation, compliance and financial protection becomes clear.

Therein lies the plan.

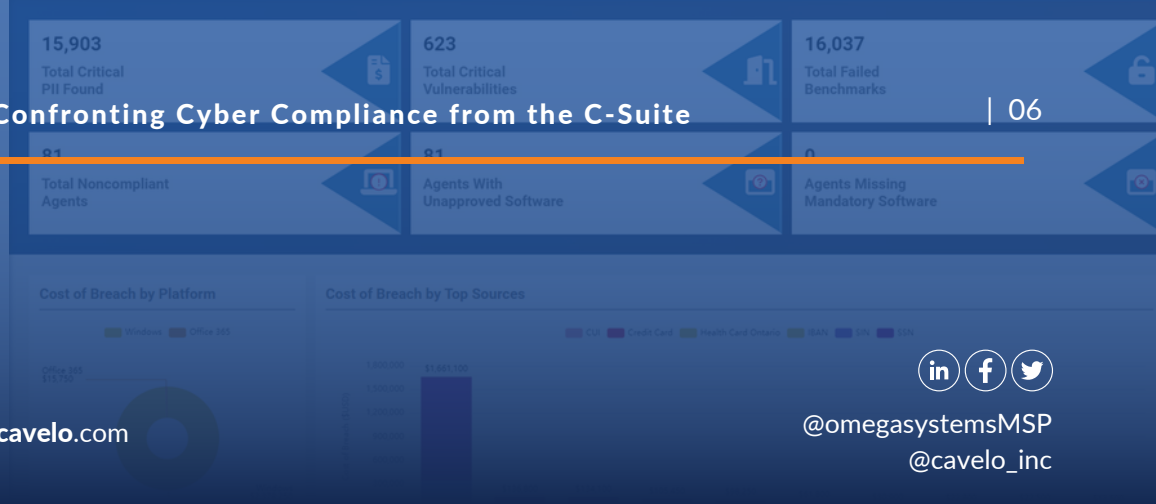


“Without real-time visibility to the business's growing inventory of digital assets and the sensitive data they contain, teams can't confidently assess and address the organization's overall attack surface and risks that are unique to the business.”

— James Mignacca, Cavelo



omegasystemscorp.com | cavelo.com

@omegasystemsMSP
@cavelo_inc

The Plan

Armed with knowledge of today's prevalent cybersecurity threats and with a realistic comprehension of the most significant hurdles to overcome, we can now assert several critical steps C-suite executives should take on their path to IT compliance.

Use Data Discovery & Classification to Guide Your Compliance Strategy

Risk management, at its core, should start with automated data discovery and classification. Yet, many businesses lack the resources needed to manage the high volumes of data that their servers, cloud applications and endpoint devices gather.

By organizing and prioritizing data based on its level of sensitivity, typical usage, regulatory applications, and other factors, IT executives gain a level of transparency to support enhancements to access control, permission structuring and specific data protection methods.

Meanwhile, CFOs and COOs get clear visibility into the organization's most critical risk areas and can apply a direct financial impact to said risk areas, providing tangible evidence to support the organization's cybersecurity and compliance efforts moving forward.

Get Proactive about Cyber Risk Management

In more cases than not, when a breach occurs, it's already too late for the business to recover. That's because most organizations have yet to enable truly proactive cybersecurity risk management programs that build in layers of protection at both the prevention (pre-breach) and recovery (post-breach) stages.


"It's impossible for businesses to protect the data they don't know about. Gaining visibility to the full scope of their sensitive data helps IT, security and compliance professionals identify, classify data and improve the hygiene of their data, thereby reducing the risk of data exposure and regulatory fines."

– James Mignacca, Cavelo

With early insight into your business's unique risks and IT environment, C-suite executives can pinpoint where IT teams/outsourced MSPs should prioritize their time, resources and budget with regard to security and optimize standards across the organization to facilitate compliance and operational efficiency BEFORE a cybersecurity incident or breach ever occurs.

Because of the ever-increasing regulatory standards permeating through various industries (e.g. SEC in financial services, HIPAA in healthcare, CMMC in government, GLBA in banking, etc.), it's more advantageous than ever to get a head-start on the compliance process.

Sophisticated IT compliance management platforms can automate much of the process by layering specific regulatory frameworks over business's existing data and controls to give IT and executive leaders clarity on how applicable data should be managed and stored as well as to provide transparency into the organization's overall security maturity.



"The companies with the most effective security programs are those that strategically align IT with business operations. The IT Director and/or MSSP needs a direct audience with someone making actionable decisions on behalf of the firm. Otherwise, the gaps within your walls are going to start to crack."

— Rick Mutzel, Omega Systems

Infuse Compliance and Risk Management into Your Financial & Operational Strategy

Risk management is not an IT problem or priority; it's an organizational one, which is why it's imperative that CFOs, COOs and other executives take active roles to safeguard the business from internal and external threats as well as financial and reputational harm.

With additional preparation and oversight of the IT compliance process, leaders can reduce security gaps as well as the costs associated with the necessary remediation and compliance penalties. Additionally, proactive, strategic compliance and risk management practices can help to reduce the cost and overhead associated with third party audits by streamlining the preparation and execution of your compliance — particularly as it applies to the time and effort needed on the part of your internal IT and cybersecurity resources.



Final Thoughts

The world of compliance is changing fast, and operational and financial leaders need to be prepared to play a role in the design and management of corporate compliance programs. Regardless of what regulatory framework you currently or will soon need to comply with, consider effective IT compliance as a way to achieve:

- Further trust among your investors, customers and employees
- More efficient resource management (e.g. less time navigating audits, remediating issues and misappropriating IT resources)
- Technology budget transparency and alignment with strategic risks and objectives

By automating the discovery and classification process and taking a strategic approach to risk and compliance management, you help ensure consistent data protection across your IT environment – and enable a robust, reliable compliance process that delivers continuous alignment with applicable regulatory frameworks and increasing stakeholder demands.

Omega Systems and Cavelo are committed to helping today's businesses navigate the complexities of the cybersecurity compliance process with ease and efficiency.

To learn more about quantifying your financial risk and driving IT compliance from an organizational level, please connect with us.

