Scrut Automation

The Role of the CFO in Cybersecurity

Scrut Automation

Contents

Introduction

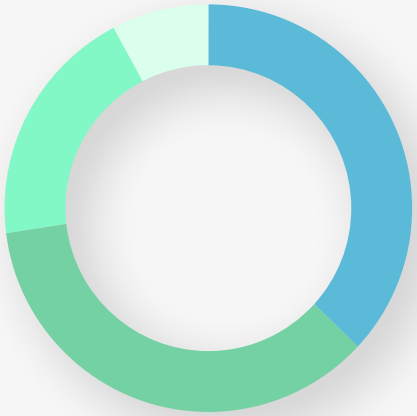
In some businesses, the Chief Financial Officer (CFO) plays a very significant role and may actually be in charge of security overall. In other instances, the Chief Information Security Officer (CISO) might be expected to report up to the CFO. This paper explores the role of a CFO in an organization's security posture.

It looks at reasons why the CFO should be one of the principal executives in cybersecurity. The CFO's fiduciary role, for example, which involves protecting corporate assets from cyber risk, often provides a compelling reason for this executive to be the primary cybersecurity leader.

Other factors include the CFO's responsibility to protect financial data and operational systems. From there, this paper offers some recommended practices the CFO can follow to be successful at the work of cyber defense.

Scrut Automation

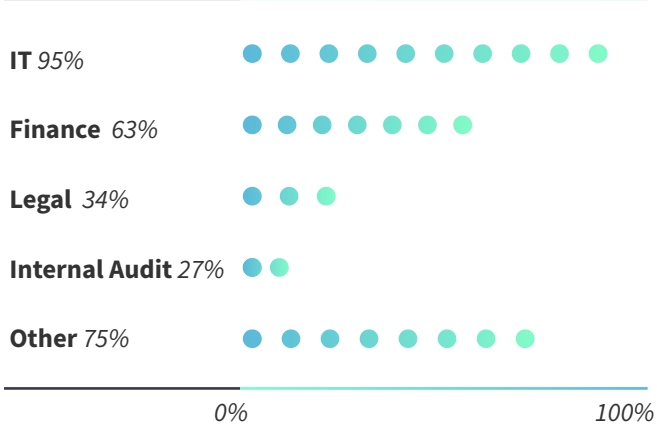
CFOs and Cybersecurity by the Numbers



Who is responsible for cybersecurity?

- CFO **38%**
- Other **19%**
- CIO **36%**
- CISO **7%**

Which departments are involved with cybersecurity efforts?



A Grant Thorton survey of members of Financial Executives International (FEI) revealed

38% CFO was responsible for security

40% CFO reported to board of directors on cybersecurity matters

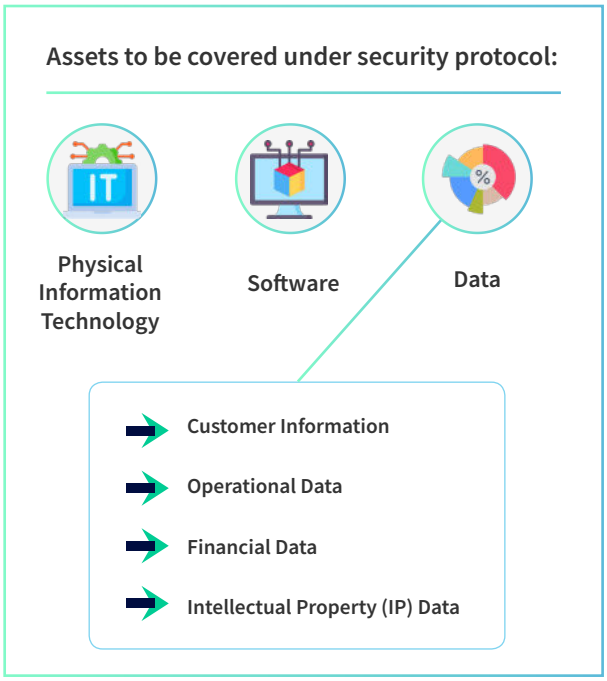
63% Finance department was involved in cybersecurity efforts

Cybersecurity and the CFO's Fiduciary Role

Why would the CFO be put in charge of cybersecurity? Managing a company's finances and defending it against hackers might seem to be quite different skillsets and areas of executive focus. However, the two are not as far apart as one might think, especially taking the CFO's fiduciary role into account.

All executives of a corporation have a fiduciary duty to safeguard the company's assets from risk. This is the foundation of risk management as a whole. Assessing risks, such as credit risk, regulatory risk, legal liability, and so forth, is all about determining what can threaten to reduce the value of a company's assets and taking steps to mitigate those threats. The CFO, in particular, has to focus on protecting assets, which are owned by the shareholders, from risk. This duty applies to digital assets, as well.

The CFO's job involves protecting valuable digital assets from harm. Examples of digital assets range from physical information technology (IT) infrastructure and software to data. Data is arguably one of the most valuable assets for the modern company. It is an asset class that includes everything from customer information, operational data, financial data, to intellectual property (IP) data. If a malicious actor can steal or damage these data assets, the company will suffer a loss of asset value.



Damage to digital assets can result in actual costs, such as the expenses of remediating a data breach—a process that can easily run into millions of dollars—as well as effects on share price based on public perceptions of a company's trustworthiness and the quality of its operations. Regulatory penalties can also arise from damage to data assets, such as databases that contain personal identifiable information (PII). The CFO is, or should be, the main person on point to deal with these risks.

The CFO's Duty to Manage Risk

The CFO's duty to protect shareholder assets translates into a duty to manage digital risk. This may involve quantifying risk to digital assets in financial terms. While in an earlier time, quantifying cyber risk was largely a matter of guesswork, it is now possible to estimate the actual costs of different kinds of cyberattacks. These costs vary by industry.

For example, a breach of customer data may be more expensive to remediate at a regulated financial services firm than it would be at a retailer. Based on industry peer data, coupled with data from cyber insurance carriers, risk quantification tools can put a dollar figure on each type of cyber risk a company is facing.

The result of this process is a report to the CFO that might say, for example, that the highest-priced risk the company faces is from a denial of service (DoS) attack that would interrupt operations. The second most costly attack would be a breach of IP data, and so forth. Imagine that these top two risks have price tags of $10 million and $5 million respectively. Armed with that information, the CFO will then have the basis to decide if cybersecurity requires a proposed budget of $10 million. Given the potential cost of risks, the budget might look very reasonable.

This example again shows the value of placing the CFO in a key cybersecurity leadership role. He or she is tasked with making critical financial decisions. Dealing with cybersecurity is, among other things, a matter of money.

Key Responsibilities

- Quantifying risk to digital assets in financial terms
- Decisions on cybersecurity budget

Scrut Automation

The CFO's Role in Protecting Systems and Data

The CFO is also in charge, at least in departmental terms, of a company's financial systems. At large companies today, this almost always means enterprise resource planning (ERP) systems that handle accounting and financial management, as well as operational functions like warehouse management, sales order management, and so forth. Indeed, almost all major systems at a business link directly to its financial systems. A disruption to that financial management system is a disruption to the business as a whole. For this reason, the CFO should have a role in defending those systems from attack.

Financial operations are also within the CFO's management domain. This includes workloads like accounts payable, accounts receivable, cash management, and payroll. These operations depend on systems and data, which are vulnerable to attack. If a malicious actor can cause financial operations to cease, he is effectively paralyzing the business. This might not be a major issue if the delay is short-lived, but if a major company cannot pay its bills or its employees for more than a few days, there could be serious consequences.

A related risk is the potential for a business to face email fraud, a form of cyberattack that has hackers pretending to be a company's CEO or CFO and ordering employees to make bank transfers. This might sound far-fetched, but one might be shocked at the global firms that have been swindled out of millions of dollars from this practice. The CFO needs to protect his or her department from being victimized like that.

Key Responsibilities

- Safeguarding financial management system
- Risk mitigation of financial operations
- Protect organization from email fraud

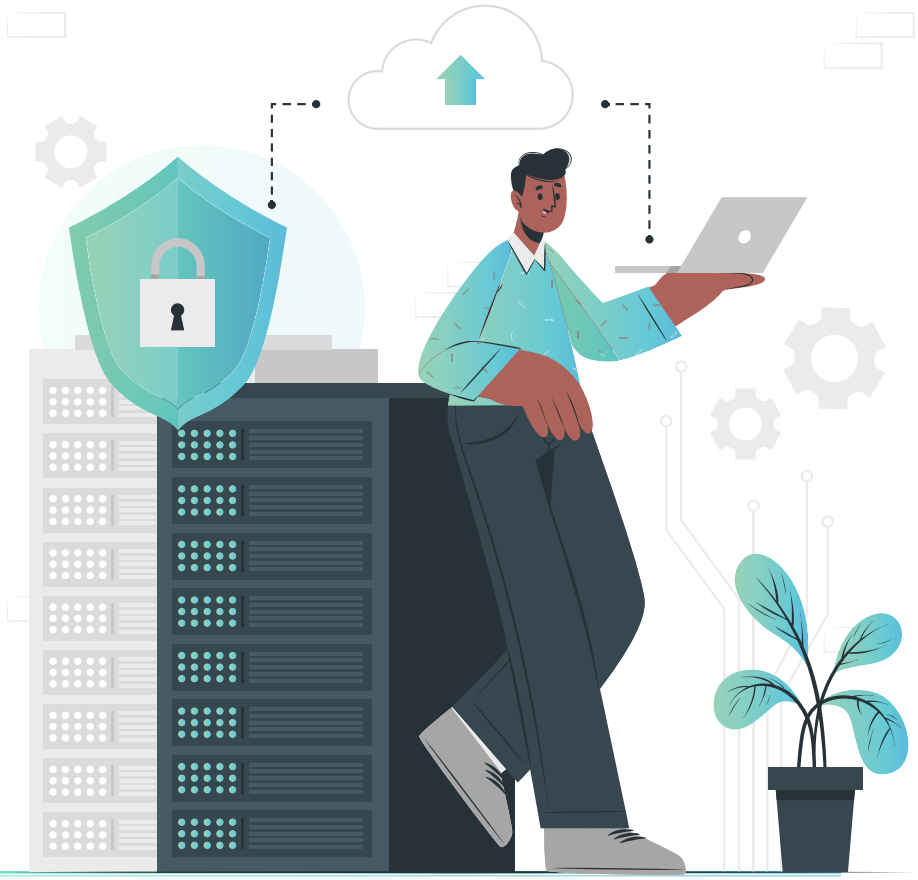
The CFO as Buyer-in-Chief

Cybersecurity solutions cost money, a fact that gives the CFO a voice in their procurement. Typically, the CFO is not the main decision maker for a security purchase, but he or she is the one who signs the check, so to speak. In many cases, the stakeholders who want to buy a certain cybersecurity tool will need to justify it, in financial terms, to the CFO.

For example, will security orchestration, automation and response (SOAR) enable the cybersecurity team to reduce headcount, and therefore save money—while improving security posture at the same time? The CFO will have an opinion about that question, which will affect the purchasing decision. Or, will a new governance, risk management and compliance (GRC) solution reduce the likelihood of paying out penalties? The CFO will want to hear how champions of the new GRC solution will make their case.

Key Responsibilities

- Key influencer for security purchases
- Weigh options and lead purchase decisions



Scrut Automation

Why the Security Team should Report to the CFO

Some companies struggle with where to place the cybersecurity team in the organization. Experts tend to agree that cybersecurity should not be part of the IT department, due to potential conflicts of interest. With this organizational setup, the IT leadership may have an incentive to minimize security risks that are occurring on their watch.

As a result, a company may establish cybersecurity as a freestanding department reporting to the CEO, or even straight to the board of directors. This is not always ideal, especially in a large organization. It may be preferable to have the security team and Chief Information Security Officer (CISO) report to the CFO. As the risk management duties outlined in this paper make clear, the CFO has a compelling reason to be in charge of security.

How the CFO Can Best Execute Their Cybersecurity Role

Some CFOs get hired into a role that includes cybersecurity. They may decide they don't want the responsibility, though some involvement is probably wise. Other times, the CFO joins the executive team with no security duties, so he or she might want to become part of the security leadership. As a CFO takes on a security role, however, he or she needs to figure out the best way to make a positive impact the organization's security posture.

Establishing and overseeing enterprise-wide workloads

The CFO needs to determine where, exactly the finance department has a role to play in cybersecurity and where it may be best to let others handle the work. While yes, the CFO has an overall duty for security, that does not mean that finance teams should be weighing in on issues like firewall settings and authentication tokens. Instead, the best approach is to look at enterprise-wide workloads and choose areas that most affect finance, such as ERP system administration and revenue-facing application programming interfaces (APIs). These are areas where the CFO should have a voice. A "heat map" process can identify the most relevant areas of operations, i.e., where a cyber incident would have the greatest impact on finance and business operations.

Taking a multidisciplinary approach to security

Cybersecurity programs work best when they are multidisciplinary in nature. The security team should collaborate with partners from IT, business management, human resources, finance, compliance, and legal. If this is not the way a company is doing things, the CFO should ideally step up and suggest such an approach.

Creating teams and task forces

The CFO is an individual, so he or she cannot—and should not—be personally involved in every aspect of the finance department's cybersecurity workloads. The CFO should create teams and task forces to oversee and implement various security-related projects and programs. Some may be temporary, such as a team that selects a new GRC tool. Others will be permanent, such as a team that reviews IT controls for financial systems.

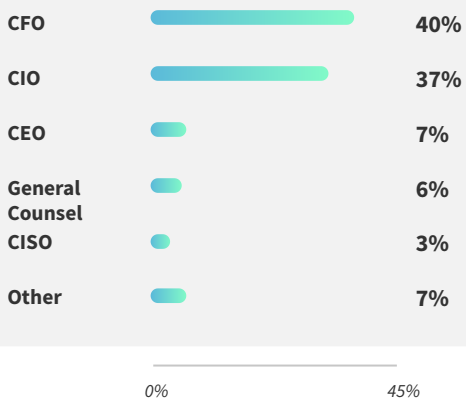
Having a voice in security-related decisions and operations

The CFO should insist on having representatives of his or her department involved in security-related decisions and operations. This may be part of a multi-disciplinary approach to security, but even if the organization has not embraced multidisciplinary cybersecurity processes, finance still needs to have its voice heard when it comes to matters affecting finance and business risk.

Reporting to the board

Opinions vary on who should be responsible for reporting to the board of directors about cybersecurity matters. If the CISO does not report to the CFO, then it should be the CISO who communicates with the board. Otherwise, the CFO is the best candidate for the job. He or she can speak to the critical relationship between cybersecurity, finance, and the defense of corporate assets against threats. The CFO is also well positioned to address board questions about investments in cybersecurity and whether they are justified by financial considerations.

Who is responsible for reporting to the board about cybersecurity?



Source: Grant Thornton survey

Conclusion

At first glance it may seem that the CFO does not have much connection to cybersecurity. In reality, the CFO can, and should have an important role to play in cybersecurity. At some companies, the CFO is entirely in charge of cybersecurity. Most of the time, the CFO is involved in security and has a voice in areas of decision making and operations where cyber risk and financial management intersect. Ultimately, it's about protecting digital assets, such as data, from risk. The CFO bears this responsibility, so he or she should advocate for engagement in cybersecurity. The best practice is to take a multidisciplinary approach, building teams that can make the finance department a significant stakeholder in cybersecurity.

But how can a CFO streamline the cybersecurity operations to reduce overload? By automating them. Scrut's smartGRC is a built-in partner for CFOs who are looking for an automation solution that will continuously scan their organization's cloud environment and help them build a secure network. The risk management module on Scrut's dashboard will also enable CISOs to proactively remediate cybersecurity risks and gain visibility of their organization's security posture.