The State of the 2022 CISO

BARR ADVISORY

Table of Contents

Introduction

Cyberattacks are at an all-time high. According to the Identity Theft Resource Center's 2021 Data Breach Report, the number of reported data breaches increased by 68% from the previous year. Not only are data breaches increasing in frequency, but the cost of data breaches has increased, too. According to IBM, the average cost of a data breach in 2021 was $4.24 million.

The increase in cyberattacks can be directly linked to the accelerated shift online due to the pandemic, in addition to the already existing threats as the IT world shifts even more to the cloud. Within a matter of days, organizations and their employees shifted to remote work in early 2020, relying on the cloud to make it possible. Given the constantly changing threat landscape, particularly over the past few years, companies of all sizes need to develop a strong cybersecurity program. For mature organizations, that's where the Chief Information Security Officer (CISO) comes in. But what does a CISO actually do?

Over the past few decades, the role of the CISO has evolved to meet cybersecurity needs, and is now more important than ever before. With emerging technologies, continued adoption of the cloud, and a rapidly changing industry, the responsibilities of a CISO have grown to encompass a wide variety of responsibilities. Defining the role of a CISO is a complex challenge, especially when many stakeholders may not realize the intricacy and value of the security professional's role.

The CISO is ultimately responsible for the confidentiality, integrity, and availability of a company's information assets, including data and systems. The CISO should have a seat at the table for all critical projects. An effective security officer leverages the authority they have to ensure security is applied to all projects, particularly IT and software development projects.

This whitepaper utilized the 2022 CISO MindMap, developed by Rafeeq Rehman, to simplify the roles and responsibilities of a CISO.

Risk Management

An effective CISO understands how to identify and mitigate information risk within an organization. They know how to apply information risk in a more holistic manner because they understand how information risk applies to the rest of the business. They know how to mitigate information security risks in the context of the entire organization.

The risk management aspect of the CISO role includes all of the threat prevention responsibilities such as vulnerability management, but also incorporates broader risk-related tasks. Properly educating employees on how to recognize phishing emails and other potential scams, for example, is an important part of mitigating internal threats. Other buckets of this risk management responsibility include conducting ongoing risk assessments with inputs from risk assessment-adjective activities like penetration testing, code reviews, implementing strong policies and procedures, and appropriately managing Internet of Things (IoT) devices.

Risk management responsibilities for a CISO extend beyond internal efforts. In a study conducted by Experian, 50 percent of respondents said that data breaches at their organization were a direct result of a third party incident. Evaluating third party risk is essential. It's important for a CISO to take a data-centric approach to vendor security reports and understand who has access to their organization's data, control that access, and prevent data loss or theft as a result of that access. A CISO is also responsible for responding to third party security vendor questionnaires—a process that can be automated for efficiency.

A study conducted by Experian found that

50%

of data breaches were a direct result of a third party incident

Governance and Compliance

A CISO is responsible for aligning security processes with the rest of the business to support the organization's overall strategy. This includes resource management, defining accountability for security within the organization, and overall risk management.

As the leader of information security, a CISO ensures that their organization meets compliance regulations relevant to their organization. As their organization undergoes regular audits, a CISO will ensure their security controls are in compliance with necessary frameworks and regulations. This may include:

- GDPR, Microsoft DPR, and/or other data privacy regulations
- PCI DSS
- SOC 2
- HIPAA/HITECH
- HITRUST
- ISO 27001
- NIST 800-53, 800-171, and CSF

Business Enablement

While security operations and risk management seem like obvious aspects of the CISO role, today's CISOs are also finding themselves responsible for achieving business objectives. Security and risk have become inherently connected to business enablement as the increasing threat of cyberattacks has become a reality for organizations of all sizes. In addition to deep technical knowledge and skill, business acumen is a crucial skill for every CISO.

Business enablement for the CISO looks a little different than it does for other C-Suite executives. Instead of being solely responsible for business growth, the CISO is responsible for securing the people, processes, and technology that create growth opportunities. This includes HR processes, like ensuring onboarded employees have access to the necessary data for their role and terminated employees do not have access to company files. If associates are using their mobile phones from work, a CISO is responsible for a mobile device policy that protects their organization's data. If their company was involved in mergers and acquisitions, the CISO would be responsible for conducting an acquisition risk assessment, determining the cost and feasibility of integration, and identity management

The CISO is responsible for securing the people, processes, and technology that create growth opportunities.

Another part of business enablement for the CISO is understanding key industry trends and evaluating emerging technologies. In order to stay competitive and secure, a CISO is responsible for understanding how the latest news and technologies will impact their organization.

Security Operations

Running security operations is one of the key responsibilities of the CISO and their team. The CISO is responsible for developing, implementing, and managing an information security operations program. This category can be defined by three main buckets: threat prevention, threat detection, and incident response and management.

Threat Prevention

Threat prevention is the strategy of defending your network and systems by preventing threats from affecting your organization. This includes network firewalls that secure the perimeter, managing and patching vulnerabilities, application security, encryption, and more. Threat prevention strategies are often made up of a number of different policies and tools. Vulnerability scans and penetration tests are two examples of threat prevention strategies.

Threat Detection

Threat detection, on the other hand, is the strategy of identifying and remediating any malicious threats before it can exploit or otherwise compromise your network. This includes log analysis, creating a process for alerting the team when a threat is discovered, threat hunting and mitigating insider threats, and using other defensive strategies to mitigate known and unknown threats. A well-oiled security operations team should be prepared to quickly detect and respond to threats before attackers are able to take advantage of it. Threat detection and prevention go hand-in-hand: a comprehensive security program will include robust processes under each category. They complement each other and help identify weaknesses in the other.

Security Operations

Incident Response and Management

The CISO is also responsible for incident response and management. This means having an adequate incident response plan in place in the event of an event that impacts the confidentiality, availability, or integrity of information assets. For most organizations, a security incident isn't a matter of if but when, making preparation for an eventual breach a critical aspect of security operations. This may involve preparing forensic investigations, undergoing an incident readiness assessment, purchasing a cybersecurity insurance policy, and creating a business continuity plan and internal communications strategy. Additionally, the CISO should be prepared to work with a crisis communications specialist to notify any impacted parties in a timely manner, and brief the media if necessary. A breach response plan should also be tested with breach simulations, such as red team and tabletop exercises, to ensure that the plan is adequately designed.

When it comes to incident management, ransomware is currently top-of-mind for many CISOs given the recent increase in ransomware attacks to companies and critical infrastructure. According to IBM's Cost of a Data Breach Report, the cost of ransomware attacks is more expensive than the average data breach, costing businesses an average of $4.62 million. Because of this, CISOs are often responsible for developing specific ransomware response plans as part of their incident management strategy. Ransomware should be included in any incident response drill an organization performs. This provides a detailed guide for security and technology teams to follow in the event of a ransomware attack.

Budget

Every company needs to budget for security, and the CISO can help advise the leadership team on how much money their organization should spend on cybersecurity. Figuring out how much to budget for cybersecurity begins with asking how much the organization values their data. A CISO will guide their organization through appropriate risk assessments and threat modeling to determine their security priorities. It's the CISO's job to clearly communicate to executives the importance of security and the resources required to secure the organization's information assets so as to ensure executives are willing to provide those resources.

When allocating a budget, a CISO will assess the necessary security and automation tools, technology, and training that aligns with the organization's security priorities. While cybersecurity is often a hefty investment for many organizations, security spending can directly link to revenue—organizations want to work with companies that value security and will protect their data. Companies that value information security and invest in it, often see returns in the form of increased sales and shortened sales cycles.

CISO Budget Considerations

- Tools
- Technology
- Training

Identity and Access Management

Identity management may seem like a simple part of a CISO's job, but this responsibility has a big impact on the CISO role. According to IBM, compromised credentials are the most common cause of a data breach. Breaches resulting from compromised credentials take significantly longer to detect compared to other breaches.

With this in mind, a CISO is responsible for implementing and managing procedures that secure employee identities. This includes account creation and deletion, multi-factor authentication (MFA), role-based access control, password resets, and more.

CISO Procedures to Secure Employee Identities include:

- Account creation and deletion
- Multi-factor authentication (MFA)
- Role-based access control
- Password resets

The CISO and their team closely collaborate with software developers to ensure that cybersecurity is an integral part of project lifecycles. A CISO can ensure that software projects meet all security requirements. The security team typically reviews design and conducts security testing as part of the project management schedule.

Legal and Human Resources

The CISO role also has overlap with legal and human resources, and working closely together with them is an important part of this position. Onboarding or terminating an employee comes with inherent ties to security, especially with regard to access management.

A CISO will work closely with the legal team on important business endeavors, such as regulations and compliance efforts and third party vendor contract management. Since a CISO is responsible for ensuring the security and managing the risks associated with vendor relationships, they will need to make sure that all legal contracts appropriately align with security standards. In the event of a security incident or breach, legal and security teams would collaborate on appropriate and timely response. A CISO will work closely with legal departments to ensure policies and procedures, as well as business activities, align with data protection regulations such as GDPR and CCPA.

Permanent Work from Home

A study by Pew Research found that two years after the pandemic accelerated the shift to remote work for many office workers, six in 10 U.S. workers who say their jobs can mainly be done from home are still working remotely.

For many companies, particularly SaaS and other tech companies, remote work has become a permanent facet of their organization. And while remote work comes with a number of benefits, it also expands the organization's attack surface and can lead to a number of security issues.

The CISO team is responsible for mitigating security risks associated with remote work. This includes enabling secure application access, securing the expanded attack surface, and ensuring that any sensitive data accessed from home networks is secure.

Selling Infosec

While a CISO might own cybersecurity for an organization, people are the foundation of security. When everyone in the organization, from the most skilled security developer to the marketing team intern, understands what's being protected and how certain behaviors can lead to compromised security, a culture of security and compliance is created.

A CISO doesn't just feed people information about what security is and why it's important—they provide them with the necessary tools and processes to assist them. Simply providing security awareness training, while important, isn't enough. Security should be top of mind at all times and an effective CISO uses a variety of tools and processes to keep security top of mind for everyone. This includes an established process of where associates can turn with regard to specific security problems or concerns.

While the CISO can develop the organization's security practices and strategy, those practices need to be instilled and reinforced. A CISO can partner with a marketing or creative team to build a brand around the best practices for associates to relate to. They can work closely with creative teams to generate unique ideas to spread the importance of information security throughout the organization, and hopefully within the industry.

Since its inception, the responsibilities of the CISO role have steadily increased alongside rapidly changing and emerging technologies. As these responsibilities continue to evolve, having a trusted security and compliance partner like BARR Advisory can help organizations stay flexible and adaptive to the needs of its stakeholders.

About BARR Advisory

At BARR Advisory, we build trust through cyber resiliency. We help protect the world's data, people, and information networks through a human-first approach to cybersecurity and compliance. Businesses looking for the accessibility of a boutique firm with the tools and expertise of a global consulting firm will find a partner in us.

Specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud, BARR has the global network of partners, the perspective, and deep expertise every thriving SaaS provider to world-class enterprise needs to stay secure and compliant at every stage.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/ HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Virtual CISO Services**
- **People & Culture Services**

Connect with BARR

Want to learn more about the role of the CISO or if your organization could benefit from a virtual CISO? Contact us today.