eclypses

WHITE PAPER

Cyber Attacks Become Top Business Risk for U.S. Executives

What cybersecurity challenges keep business leaders awake at night?

www.eclypses.com

Document ID: Eclypses- 1532395320 - 296
Version No.: 2.0

Contents

Introduction

What keeps business executives up at night? This question comes up more often now than ever before in the cybersecurity landscape. As we see cybercrime continually increasing, governments issuing higher fines for breaches, and business executives being held accountable, there is more to worry about for business leaders.

A recent Gartner survey found that, “Eighty-eight percent of Boards of Directors (BoDs) view cybersecurity as a business risk, as opposed to a technology risk, and that only 12% of BoDs have a dedicated board-level cybersecurity committee.”

The increase in fines for serious or repeated privacy breaches extends globally, as other countries are also implementing new legislation to hold companies accountable. It was reported back in October 2022 that the Australian Federal Government will impose a significantly higher financial penalty on companies engaged in serious or repeated privacy breaches, increasing from $2.2 million to at least $50 million. (Source)

With new reports and statistics like this surfacing almost daily, it’s no wonder why the anxiety of cyber-attacks keeps CEOs awake at night. It is now more important than ever for business leadership (not only technology leaders) to take action against cyber threats now.

Business Executives Are Being Held Accountable for Cyber Attacks

Drizly is one of the largest online marketplaces for alcohol in North America and its CEO is being held accountable for data privacy abuses, following allegations that the personal information of approximately 2.5 million customers was exposed under his management. The U.S. Federal Trade Commission plans to use data privacy protection orders like the one proposed against Drizly and its CEO to hold companies responsible when they allegedly abuse or misuse customer data.

An HG.org article, states, “It is possible for a company to be held liable when the customer data stored within is hacked by an outside source. Even though the business has become the victim of a crime, it may still be accountable for the incident. This is due to the ability of the company to secure the information.”

What about the responsibility of board members ensuring their organizations operate within the law? In re Caremark case, the courts recognized a duty on the part of directors and officers to monitor corporate operations that have the potential to create liability for the company, according to a blog post from Sidley. It goes on to point out that this duty is understood as a duty of loyalty, because where directors know or should know that they have a duty to act, and they fail to do so, “they breach their duty of loyalty by failing to discharge that obligation in good faith.”

It is expected to see these cases grow as more top executives and board members are being held accountable for cyber attacks.

Types of Cyber Attacks Executives Are Most Concerned About

1. **Malware**
   Malware is malicious software that includes, spyware, ransomware, viruses, etc. Typically activated when a user clicks on a malicious link or attachment and leads to the installation of harmful software on your device.

2. **Insider Threats**
   Insider threats are when an insider uses their authorized access or understanding of the business to harm that organization. According to CISA, it can include malicious, complacent, or unintentional acts that negatively affect the integrity of confidentiality, and availability of the organization, its data, personnel, or facilities.

3. **Ransomware**
   Ransomware is when a hacker holds a company's data hostage until the victim pays a specific dollar amount. For example, in the infamous 2021 Colonial Pipeline attack, hackers breached their systems using compromised passwords and demanded approximately $4.4 million.

4. **Phishing**
   Phishing is a type of social engineering where a hacker sends deceitful messages that are designed to trick a person into divulging sensitive information to the hacker.

5. **Man-in-the-Middle**
   A man-in-the-middle (MiTM) attack is where hackers secretly intercept and relay messages between two parties who believe they are communication directly with each other. They can capture sensitive data such as credit card numbers, login credentials, financial information, etc.

The Challenges Executives Face Surrounding Regulatory Compliance

Regulatory compliance helps companies develop the foundation on which they are built, define their brand, and help to build a positive reputation. Business executives know it is critical for investors and clients to feel confident, not only in a company's product offerings but also in their behavior related to how they conduct business. Customers need to understand that the company they are working with keeps their teams aligned with compliance initiatives and always acts with integrity.

One of the biggest challenges related to regulatory compliance would be businesses staying ahead of regulatory changes year over year.

The Securities and Exchange Commission ("SEC") issued a new set of proposed cybersecurity rules for public companies in 2022, increasing the SEC's scrutiny of public companies cyber-related activities, decision-making processes, and the Board's new role in overseeing cybersecurity, according to a JDSupra article.

A company's preparation and response to a data breach can affect both civil and regulatory liability, but data security efforts and disclosure are key to mitigating that liability, according to Cincinnati Business Courier article. It has become necessary to have a strategic cybersecurity policy in place for any organization, small or large.

Looking Towards the Future

When facing the uncertainty of cybersecurity, it is essential to understand that creating a multi-layer approach to security helps keep data protected even when vulnerabilities are exposed. Setting the tone from the top by prioritizing cybersecurity throughout the entire organization is really the first step. Below are a few security strategies that should be implemented right away:

1. Provide cybersecurity training for the entire company.
2. Identify what types of sensitive data you have.
3. Utilize anti-virus and anti-malware software on all devices and networks.
4. Implement multi-factor authentication (MFA) as an added layer of security.
5. Require strong password policies.
6. Always back up your data.
7. Fully understand your cyber insurance policy.
8. Move away from session-based zero-knowledge security sessions.
9. Use endpoint security solutions that replace data at the application level, securing data before it gets to the operating system and protects through any network until delivery to the receiving application.

> *"With zero-day attacks and credential stuffing attacks increasing at an alarming rate, traditional security is unable to protect an organization's data (and their customer's data) the way we need it to. When looking for a data security solution, it's essential to look for a technology that verifies each endpoint connection, requires no change to the user experience, has minimal impact on system resources, secures data inside the application, and allows you to stop trusting the operating system and communication protocol."*
>
> *- Tim Reynolds, Chief Development Officer at Eclypses*

Conclusion

In the past CEOs, Board Members, etc. have not always had cybersecurity set as a priority. Today we are seeing the shift take place where cybersecurity is becoming a necessary part of how companies operate. With a 68% increase from the year before, the Identity Theft Resource Center's 2021 Data Breach Report cited there were 1,862 breaches last year. Top executives cannot ignore the fact that it's not a matter of whether their organization will be hacked – it's just a matter of when.

To learn more about how executives can protect their organization's sensitive data, reach out to Eclypses at contact@eclypses.com.

Sources

1. Identity Theft Resource Center. (2022, January 21). Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises. ITRC. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

2. Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as. (2021, November 18). Gartner. https://www.gartner.com/en/newsroom/press-releases/2021-11-18-gartner-survey-finds-88-percent-of-boards-of-directors-view-cybersecurity-as-a-business-risk

3. Optus and Medibank hacks prompt government to increase fines for massive data breaches to a minimum of $50 million. (2022, October 21). ABC News. https://www.abc.net.au/news/2022-10-21/data-breach-fines-increase-after-medibank-optus-hacks/101564614?

4. Zakrzewski, C. (2022, October 24). FTC brings action against CEO of alcohol delivery company over data breach. Washington Post. https://www.washingtonpost.com/technology/2022/10/24/ftc-drizly-privacy-violations/

5. Security Breach - How Businesses May Be Liable. (n.d.). www.hg.org. Retrieved December 4, 2022, from https://www.hg.org/legal-articles/security-breach-how-businesses-may-be-liable-44358

6. SEC Proposed Cybersecurity Rules – What They Are and What Our Clients Should be Doing Now. (n.d.). JD Supra. https://www.jdsupra.com/legalnews/sec-proposed-cybersecurity-rules-what-2345066/

7. Prescient. (2019, May 3). Top 5 Cyber Security Threats for Executives. Retrieved December 8, 2022, from https://www.prescient.com/blog/cyber-security-threats-executives/

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies, websites, and IoT devices. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

This technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT

contact@eclypses.com
www.eclypses.com
(719) 323-6680