Focus On...

Helping you bring your organization into focus.™

October 2020 • Volume 10, Issue 10

CYBER

Threat of Fines Drives Board Decisions on Cybersecurity Spend

Thycotic, provider of privileged access management (PAM) solutions, released its CISO Decisions survey, an independent global study that examines what most influences the Board to invest in cybersecurity and the impact this has on CISO decision-making.

Based on findings from more than 900 global CISOs/Senior IT decision-makers, the research shows Boardroom investments in cybersecurity are most commonly the result of an incident or fears of compliance audit failure. Because of this, the research shows more than half, 58 percent, of respondents say their organizations plan to add more towards security budgets in the next 12 months.

There are positive signs that Boards are stepping up with investment. More than three quarters (77%) of respondents have received Boardroom investment for new security projects either in response to a cyber incident in their organization (49%) or through fear of audit failure (28%).

COVID-19 Drives More Security Investment

Amid growing cyber threats and rising risks through the COVID-19 crisis, CISOs report that boards are listening and stepping up with increased budgets for cybersecurity, with the overwhelming majority, 91 percent agreeing that the Board adequately supports them with investment. Almost 3-in-5 believe that in the next financial year they will have more security budget because of COVID-19.

CISO Challenges Still Exist

However, CISOs have their work cut out to gain the Board's support. Almost two fifths (37%) of participants' proposed investments were turned down because the threat was perceived as low risk or because the technology had a lack of demonstrable ROI. One third (33%) believe senior management does not comprehend the scale of threats when making cybersecurity investment decisions.

CISOs Think Strategically But Invest Tactically

CISOs' own approaches to buying decisions are forward looking as they try to keep up with industry developments and their sector peers. An overwhelming majority (75%)

Inside This Issue

***Cyber:* Threat of Fines Drives Board Decisions on Cybersecurity Spend**

***Compliance:* Pandemic Brings Increased Compliance Risk**

***Awareness:* Fake News**

Focus Audits will be closed on Monday, October 12, 2020 in observance of Columbus Day.

FOCUS AUDITS™

CYBER

> ***"Securing Boardroom investment requires [CISOs] to strike a delicate balance between innovation and compliance."***
>
> ***James Legg, CEO at Thycotic***

say they want to try out innovative new tools. However, in practice, they are guided by their industry peers, with almost half (46%) benchmarking their buying decisions against other companies in their sector. This may lead CISOs to err on the side of proven known technology rather than trying something new.

"Our study clearly shows that before CISOs' can pursue technology innovation they must first educate their stakeholders about the value of cybersecurity," said James Legg, CEO at Thycotic. "Securing Boardroom investment requires them to strike a delicate balance between innovation and compliance."

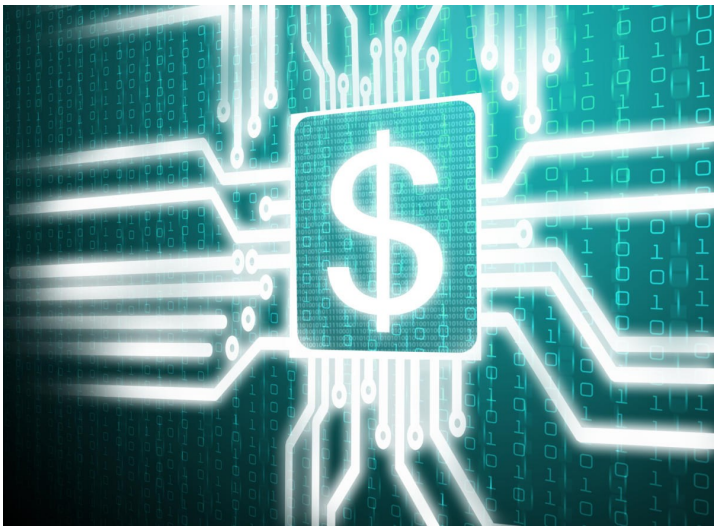
This balance is discernible in the way decision-makers describe their organization's risk profile. Almost half of respondents view their organization as 'in the pack' (45%) and only a third consider their companies to be 'pioneers' (36%), embracing new technology advancements. Only 17 percent think their business has its finger on the pulse, prioritizing investments according to the latest security threat.

"While boards are definitely listening and stepping up with increased budget for cybersecurity, they tend to view any investment as a cost rather than adding business value," said Terence Jackson, CISO at Thycotic.

"The fact that Boards mainly approve investments after a security incident, or through fear of regulatory penalties for non-compliance, shows that cybersecurity investment decisions are more about insurance than about any desire to lead the field which, in the long run, limits the industry's ability to keep pace with the cybercriminals."

Thycotic's CISO Decisions survey was conducted among 908 Senior IT security decision-makers working within organizations with 500+ employees. The interviews were conducted online by Sapio Research in August 2020 using an email invitation and an online survey.

Source: ***Security Magazine, October 8, 2020***



Focus On...

COMPLIANCE

Pandemic Brings Increased Compliance Risk

The Office of the Comptroller of the Currency recently published its Semiannual Risk Perspective Spring 2020. The report was prepared from April to June and clearly indicates that Compliance risk is elevated due to a combination of altered operations, employees working remotely, and the requirement to operationalize new federal, state, and propriety programs designed to support consumers such as the CARES Act, Paycheck Protection Program (PPP), and a variety of forbearance and deferred payment programs.

These factors can create challenges for full and accurate implementation of bank policies to fulfill Bank Secrecy Act (BSA), consumer protection, and fair lending requirements. The high volume of PPP applications and the short processing time frames particularly elevate bank risks. These conditions may complicate BSA, consumer protection, and fair lending compliance responsibilities associated with underwriting and opening new accounts, monitoring customer activity, communicating with customers, and timely meeting BSA and Office of Foreign Assets Control (OFAC) reporting requirements.

Consumer Compliance and Fair Lending
Banks should follow established change management and compliance risk management processes to identify, measure, monitor, and control the emerging risks associated with the COVID-19 national emergency. Emergency-related changes in bank staffing may affect the ability of banks to comply with CARES Act provisions and other regulatory requirements. In addition, banks' strategies for processing consumer requests and applications will vary with implementation, increasing the risk of disparate treatment and disparate impact on a prohibited basis. Appropriate monitoring measures will help banks provide fair and consistent assistance and support to applicants and borrowers.

Branch closures, reduced operations, and communication issues (e.g., limited hours, lobby or location closures, and strained call center capacity) may result in increased customer complaints. Banks must remain diligent to ensure compliance with consumer protection, fair lending, and other laws and regulations when dealing with applicants for new or modified loans and working with customers affected by the COVID-19 pandemic. Additionally, the increased reliance on remote work environments may create challenges to maintaining safeguards for protecting consumers' personal financial information and for monitoring customer interactions for consistency with bank policies and procedures.

Banks are encouraged to review interagency and Consumer Financial Protection Bureau statements that provide information to banks working with borrowers affected by the COVID-19 pandemic. These statements clarify the agencies' supervisory and enforcement priorities and approaches for fair lending and other consumer protection laws during the COVID-19 pandemic.

Source: OCC Semiannual Risk Perspective Spring 2020

AWARENESS

Fake News

What is Fake News?
Generally speaking, fake news is a false narrative that is published and promoted as if it were true. Historically, fake news was usually propaganda put out by those in power to create a certain belief or support a certain position, even if it was completely false. Social media has now created an environment where anyone with an agenda can publish falsehoods as if they were truths. People can be paid to post fake news on behalf of someone else or automated programs, often called bots, can publish auto- generated fake news. The motivations as to why people create and distribute fake news are as numerous as there are individual opinions.

The Dangers of Fake News
While some examples of fake news seem innocent or just an attempt at fun, a lot of it can be malicious and even dangerous. Fake news is created to change people's beliefs, attitudes, or perceptions, so they will ultimately change their behavior. This means if you fall into the trap of believing fake news, your beliefs and your decisions are being driven by someone else's agenda. Also, in some parts of the world, there can be legal consequences for publishing and sharing fake news.

How to Spot Fake News

So how do you protect yourself from fake news? The most effective way is to only trust something once you can verify it.

- ***Consider the Source:*** Think about the actual source of the news. A local blog will not be as trustworthy as a major academic journal. What does the source stand for? What are their objectives?

- ***Supporting Sources:*** Look at the sources cited in the article. Are they themselves credible? Do they even exist?

- ***Multiple Sources:*** Don't just rely on a single article. The more you read from various sources, the more likely you can draw accurate conclusions. Also consider diverse sources and perspectives, for example, news from different countries or authors with different backgrounds.

- ***Check the Author:*** Who is the author? Research them to see if they are a credible author, their reputation in the community, whether they have a specific agenda, or if the person posting a real person. Are they authoring within their field of expertise?

- ***Check the Date:*** Make sure that the date is recent and that it is not an older story simply rehashed.

- ***Comments:*** Even if the article, video, or post is legitimate, be careful of comments posted in response. Quite often links or comments posted in response can be auto-generated by bots or by people hired to put out bad, confusing, or false information.

- ***Check Your Biases:*** Be objective. Could your own biases influence your response to the article? A problem that we humans often run into is that we only read sources that simply confirm what we already believe in. Challenge yourself by reading other sources you normally would not review.

- ***Check the Funding:*** Even legitimate publications have sponsors and advertisers who can influence an article or source. Check to see if the article is funded, and if so by whom.

- ***Repost carefully:*** Fake news relies on believers to repost, retweet, or otherwise forward false information. If you're uncertain as to the authenticity of an article, think twice or hold off on sharing it with others.

Conclusion
In today's fast-paced world of social media, fake news surrounds us every day. If you are not careful, you run the risk of believing and acting upon it. Take the time to follow these basic steps to help ensure you make informed decisions based on facts.

Source: *SANS Ouch! Newsletter, Jason Jordaan, Principal Forensic Analyst, DFIRLABS*

Focus Audits, LLC
11301 N. US Hwy. 301
Ste. 105
Thonotosassa, FL 33592
(813) 638-8565
www.FocusAudits.com