CYBERSECURITY

By Sarah Walker-Leptich

walkrinthecloud.com | sarah@walkrinthecloud.com

An interpretation of thoughts covered by authors of the Harvard Business Review series on cybersecurity.

CHAPTERS

INTRODUCTION

Cybersecurity is not just a fancy buzzword or the annoying reason you need to reset your password every two months. It is also not just some fourteen-year-old hacker in his parents' basement trying to steal people's "mystical" bitcoins or CryptoKitties[1], an NFT game where people have spent over 1 million dollars on virtual cats[2]. Cyber attackers are more likely highly intelligent and organized, sometimes even government agencies.

The reality is that cybersecurity affects us all, from cringe-worthy stunts like hacking into baby monitors or smart lights to potentially catastrophic incidents like shutting down nuclear power plants or attacking a city's essential infrastructure like hydro. Connectivity has undoubtedly improved the lives of millions worldwide, but it also poses one of the greatest threats to that life.

Many people have debated the effectiveness of security in the cloud and are insistent that on-premises infrastructure is the only way to make you one-hundred percent secure. But with 46 billion connected devices in 2021[3], it is becoming more challenging to hold on to legacy applications.

"The reality is that cybersecurity affects us all, and many of us are not even aware of how to protect our data."

[1] https://www.cryptokitties.co/
[2] https://techcrunch.com/2017/12/03/people-have-spent-over-1m-buying-virtual-cats-on-the-ethereum-blockchain/
[3] https://techjury.net/blog/how-many-iot-devices-are-there/#gref

"Cyber attacks have risen by 30% since 2020"

01 CYBER ATTACKS CONTINUE TO RISE IN FREQUENCY AND COST

According to the State of Cybersecurity 2021 Report[1], cyber attacks have risen by thirty-one percent since 2020, increasing the average budget spent on security technology by eighty-five percent.

Although businesses have reported that they could block more cyber attacks year over year, the number of attacks has increased, and so has the cost of damage of the successful attacks. The average cost of a cyber attack is $133,000, and the total damage of cybercrime is expected to exceed $6 trillion in 2021[2].

[1] https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf
[2] https://www.sumologic.com/blog/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/

02 HOW BIG OF A THREAT IS CYBER WARFARE?

One of the most powerful reminders of the threat of cyber warfare was the potentially devastating attack in 2018 on a Saud Arabia petrochemical company[1]. The attack was not designed to steal important data or shut down the plant; it was meant to trigger an explosion killing employees. The only reason the deadly attack was unsuccessful was not due to state-of-the-art security software, it was merely a mistake in the attacker's code.

Taking advantage of the cloud improves operational efficiency, but can it guarantee the protection of critical infrastructures like water treatment plants or military operations. And what costs the business more, on-premises infrastructure with lower efficiency but ultimately lower security risks, or higher efficiency in the cloud with more frequent security breaches.

Cyber warfare is a real threat that continues to become a severe risk to governments. China has even removed companies like Cisco, McAfee, and Citrix Systems from their approved list of vendors to protect against the potential of cyber warfare.

"Taking advantage of the cloud improves operational efficiency, but can it guarantee the protection of critical infrastructure?"

[1] https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

03 LACK OF ORGANIZATIONAL KNOWLEDGE AND ACCOUNTABILITY

Many executive leaders do not feel confident knowing about security threats and addressing potential attacks. According to a study from the risk-management firm Strox Friedberg (now Aon), only forty-five percent of leaders actually feel responsible for protecting their companies against cyber attacks.

According to the article, Why Boards Aren't Dealing with Cyberthreats[1], by J. Yo-Jud Cheng and Boris Groysberg, executives can improve their knowledge of cybersecurity by following these best practices:

- Continuously ask difficult questions when they do not know the answer.
- Scheduling regular security debriefings at board meetings.
- Making investment asks in data security and risk management infrastructure a priority.
- Knowing when it is time to bring in external cyber-security experts.

"Schedule regular security debriefings at board meetings."

[1] https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

"95% of all security incidents were from human error."

04 ARE EMPLOYEES THE BIGGEST THREAT TO CYBERSECURITY?

Whether you have invested in the most advanced security software, employees are your number one threat yet also seem to be your biggest strength in combating cyber attacks. IBM stated that 95% of all security incidents were from human error[1], most often by an employee clicking on a link in a phishing email.

However, employee notifications are often the only reason organizations find out about attacks, by employees reporting "phishy" emails. It is good to train every employee as if they were a CISO and as if every email is a phishing scam.

[1] https://www.securitymagazine.com/articles/85601-of-successful-security-attacks-are-the-result-of-human-error

05 PRACTICAL CYBERSECURITY TRAINING REVOLVES AROUND COMMUNICATION AND SIMPLICITY

CEOs report financial profits and losses in quarterly town halls or employee all-hands, but rarely is the CIO or CISO asked to present how many phishing attacks were thwarted or the percentage of employees that still need to complete the latest security update.

In the article, The Key to Better Cybersecurity: Keep Employee Rules Simple[1], Maarten Van Horenbeeck suggests four simple ideas to increase your employee's willingness on common security issues:

Set strong defaults: I can't even begin to count how many times I've personally hit "remind me later" once a notification asks me to shut down and install the latest update. Many companies are now enforcing automatic shutdowns if an employee postpones crucial updates too often.

Ask for commitment: Sometimes, auto shutdowns are not possible and can potentially disrupt employee productivity. IT teams could send out emails when a new security update is available and ask employees to schedule time in their calendar before a specific date.

Gamified phishing simulations: Incorporating email add-ons that help employees flag phishing emails or sending fake phishing emails to your employees to help interactively build up their resilience.

Create social proof: Benefit from the fact that humans like to compare themselves to others by sending reports to employees on how their security diligence compares to the rest of the organization.

[1] https://hbr.org/2017/11/the-key-to-better-cybersecurity-keep-employee-rules-simple

06 WHEN CYBERSECURITY BECOMES A BUSINESS BLOCKER

When a company takes a security-only approach without aligning to the business's strategy, this is called Business Blocker Security[1]. This approach creates frustrated and unproductive employees that often lead to ineffective security practices. For example, when an employee is asked to change their password every two months, most people find it hard to come up with a new password that frequently, so they only change one letter or one number. Incorporating technology such as Google's Titan Security Key[2] can help tighten security than just frequent password changes.

Another example of Business Blocker Security is not creating a standard protocol for new technologies that make productivity easier, like Dropbox. Suppose a business decides to block these websites without a standardized and permitted tool in its place. In that case, employees will often find other less secure tools, resulting in shadow IT[3], creating more considerable risks.

" When employees become frustrated and unproductive because of IT measures, that is called Business Blocker Security."

[1] https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf
[2] https://store.google.com/ca/product/titan_security_key?hl=en-GB
[3] https://www.forcepoint.com/cyber-edu/shadow-it#:~:text=Shadow%20IT%20is%20the%20use,cloud%2Dbased%20applications%20and%20services.

06 THREE UNCOMFORTABLE TRUTHS ABOUT CYBERSECURITY

In an article written by Dante Disparte and Chris Furlow called, The Best Cybersecurity Investment you Make is Better Training[1]; they state three harsh realities of cyber attacks:

1. **Defense is harder than offense:** building up your castle walls is much easier than dealing with attackers once they are inside.

2. **Attackers have time on their side:** the average cyber attack goes undetected for weeks or months, giving hackers a lot of time to plan maximum destruction.

3. **Cyber attacks evolve according to Moore's law:** cyber attacks will continue to double in quantity and will become even more effective and cheaper with AI.

" Cyber attacks will continue to double in quantity and become more effective with the development of AI."

[1] https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

"Hacking back is absolutely not active defense. It's probably illegal and probably not all that effective."

08 ACTIVE DEFENSE DOES NOT NEED TO INVOLVE HACKING BACK

Though there is no consensus among experts of the definition of active defense, hacking back should not be part of your defensive play. Aggressive defense strategies include attacking hackers in their infrastructure versus an active defense strategy by only thwarting attacks that are aimed at your business.

Robert M. Lee, the co-founder of Dragos, an industrial security firm, states, "hacking back is absolutely not active defense. It's probably illegal and probably not all that effective." It is essential to consider the ethics of launching any active defense when faced with the high emotions of a cyber attack.knowledge of each skill set because it creates an appreciation of what each other brings to the table as a team.

[1] https://www.linkedin.com/in/scott-berinato-6330ba54

09 CREATE MULTIPLE INCIDENT RESPONSE PLANS WITH SIMULATED ATTACKS

Cybersecurity now has equal attention from governments like air, land, sea, and even space. The US military creates incident response plans with simulated warfare attacks, including a practice called "a day without space[1]", securing how they would operate if their GPS or PNT satellites went down by an asteroid or a cyberattack.

Businesses should prepare for "a day without service," including simulations where an AWS region goes down with major service disruptions like it did in December of 2021[2], as well as scenarios that include hackers holding your data hostage in the form of ransomware.

In his article, Why The Entire C-Suite Needs to use The Same Metrics for Cyber Risk[3], Jason J. Hoggs recommends that businesses prepare multi-scenario incident response plans that include several phases. The first phases should be preparation, detection, and analysis. Followed by containment, eradication, and recovery. He then suggests finishing with post-incident reports to measure the success and failures of each simulation.

[1] https://www.nasa.gov/pdf/609548main_Space%20Enterprise%20Council%20Briefing%20Final%20Package%20Dec%209%20updated.pdf
[2] https://www.datacenterdynamics.com/en/news/aws-us-east-1-outage-brings-down-services-around-the-world/
[3] https://hbr.org/2017/11/why-the-entire-c-suite-needs-to-use-the-same-metrics-for-cyber-risk

10 HOW LEADERS SHOULD NOT RESPOND TO CYBER ATTACKS

When a response to a cyber attack is not executed well, executives damage their relationship with their customers and their reputation as a leader.

In his article, Avoidable Mistakes Executives Continue to Make After a Data Breach[1], Bill Bourdon writes, "until more top executives begin to hold themselves accountable for cyber incidents, and learn from the mistakes others have made before, we will continue to see breaches and poor leadership in response to cyber attacks." It is a reminder that history doesn't repeat itself; people repeat history. Executives can learn from historical cyber incidents, especially those handled exceptionally poorly, like the 2017 attack on Equifax[2], which was subjected to much controversy. Including an investigation into insider trading and corruption, as many top executives dumped their stock before going public with the breach.

"When faced with responding to the public on security breaches, executives should respond in a timely manner and accept responsibility."

When faced with responding to the public on security breaches, executives should respond in a timely manner and accept accountability. The General Data Protection Regulation (GDPR) recommends seventy-two hours, an ideal metric to aspire to but unrealistic to some companies. Maintaining customer trust should also be one of an executive's top concerns. Knowing when to say 'we don't have more information at this time but want to keep communication frequent' is okay and appreciated by customers.

[1] https://hbr.org/2017/11/the-avoidable-mistakes-executives-continue-to-make-after-a-data-breach
[2] https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

CONCLUSION

In conclusion, businesses should be well prepared with an incident response plan for multiple cyber attack scenarios, including its impact on every line of business, not just the CEO and CIO. For example, CFOs should be prepared to report on potential financial losses to stockholders, and CMOs should write pre-approved press releases they can easily tweak if an attack were to occur.

ABOUT THE AUTHOR

Sarah Walker-Leptich

www.walkrinthecloud.com
sarah@walkrinthecloud.com

I'm Sarah Walker-Leptich – and I'm obsessed with the business impacts of data analytics, blockchain and AI & ML.

For 10 years, I've been a technical product and partner marketing expert, where I've focused my time on Google Cloud, AWS, and Cisco. While at Softchoice, my most favored accomplishment has been hosting the first ever customer facing AWS DeepRacer event in Canada, which taught our largest financial customers hands-on technical experience with reinforcement learning.

Outside of work, you can find me building Lego, exploring the night sky with a telescope, or with my head in a book.

WALKR inthecloud