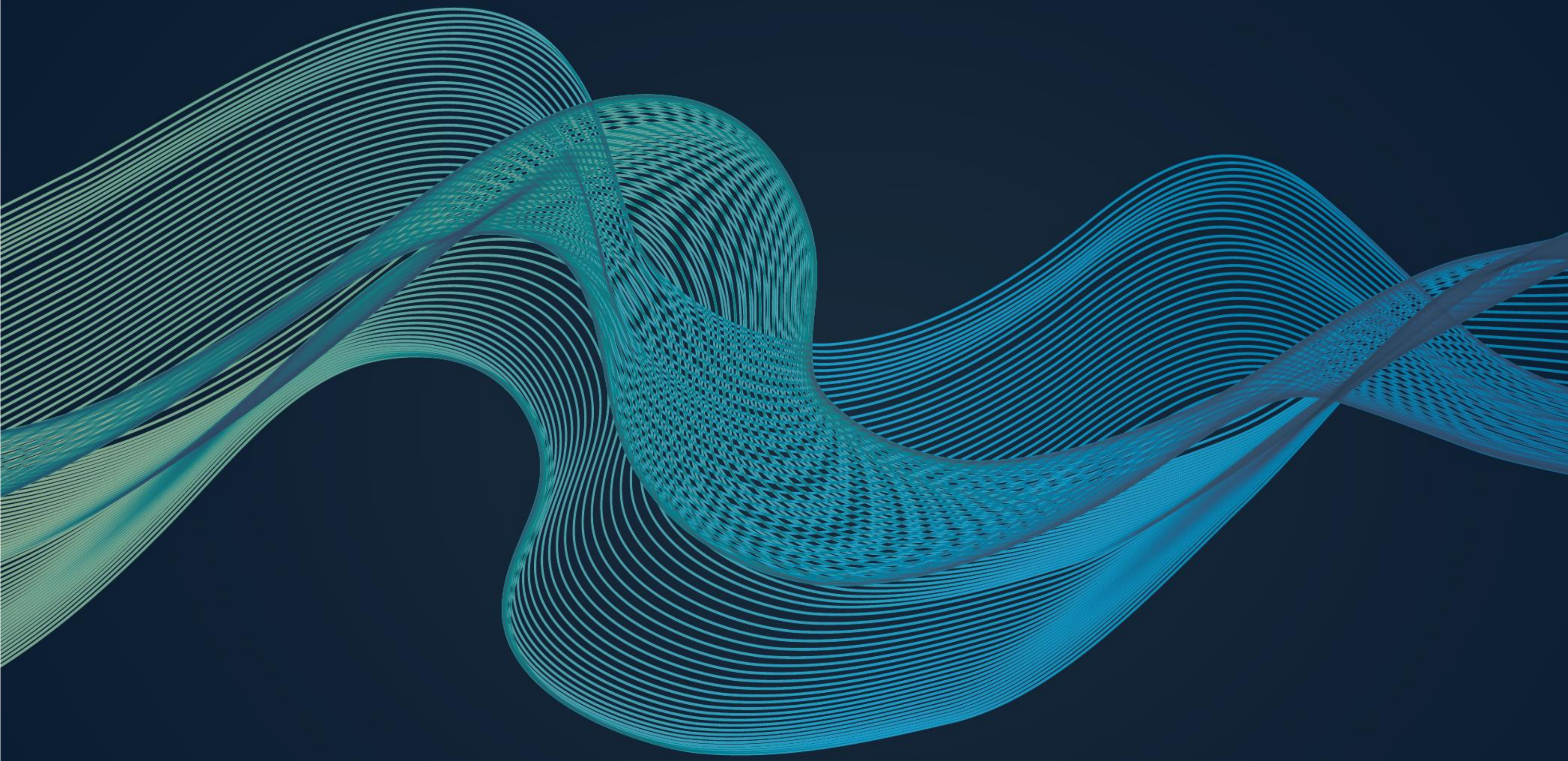
Cybersecurity and the C-Suite:

How Executives Can Understand Cyber Risks and Ensure Governance



SURFWATCH
CYBER IN SIGHT

Introduction

As cybercrime events have increasingly impacted organizations, cybersecurity has transformed from just an IT problem into a strategic issue where the C-Suite must take ownership.

In the spring of 2014, SEC Commissioner Luis Aguilar publicly stated that board members are responsible for the cyber security posture of their organizations, the first big sign that future regulation could hold organizations and their board of directors accountable for cybersecurity events. And with high profile security breaches at Target and others, corporate executives and the board of directors are now bearing the responsibility of managing the risks posed by cyber threats – and being held accountable for any attacks that slip through.

However, many executives and board members lack key knowledge about the cyber risks their organizations face and how to incorporate effective risk management decisions into their overall business strategy.

- 52% of directors ranked IT strategy and risk as the issue for which they need better information and processes – behind only strategic planning (FTI Consulting).
- Most organizations do not ensure that cybersecurity is aligned with their overall business strategy, adequately address employee and insider vulnerabilities, or assess the security practices of third-party partners and supply chains (PwC).

The impact of a cyber-attack on a business has real consequences, resulting in more than simply bad headlines and technical problems; it can lead to lost jobs, rising legal costs, non-compliance penalties, loss in brand reputation, customer loss, and ultimately a direct impact on the bottom line. But because of how cybersecurity has traditionally been managed, there is a continental divide between the technical world and the business side, where cyber risk management is not really baked into the business strategy.

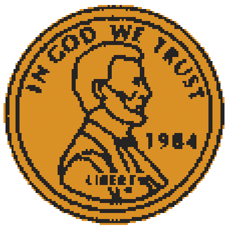
The way to bridge the gap – so that cyber problems and solutions are relevant and comprehensible to those in the C-Suite and Boardroom – is to leverage cyber risk business intelligence that can provide real insights and benchmarks to revisit as part of every business strategy session.

This paper is written for business decision-makers to help understand the risk landscape and learn how to incorporate a sound cyber risk framework that is based on a business intelligence approach.

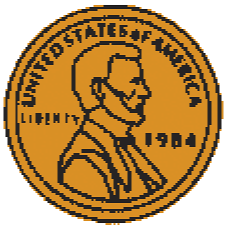
Decisions in the Dark: The Penny Test

Without a full picture of cyber risks facing an organization, it becomes easy to make mistakes. This is a problem often seen in the world of physical crime, where a lack of information can have devastating consequences. According to the Innocence Project, “Eyewitness misidentification is the single greatest cause of wrongful convictions nationwide, playing a role in 72% of convictions overturned through DNA testing.”

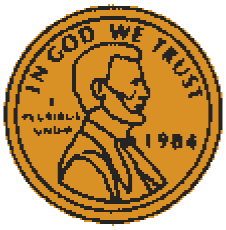
The point the organization is trying to highlight isn’t that eyewitnesses are being careless – it’s that systemic issues within organizations can lead to costly mistakes. This is illustrated with a variation of the Penny Test, using six person “lineup,” to see if you can identify the “real” penny.



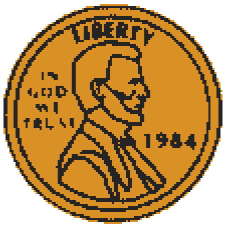
1



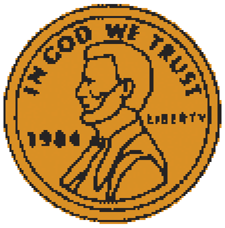
2



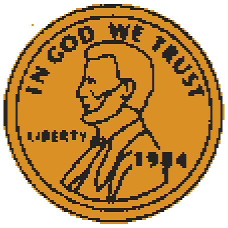
3



4



5



6

Which one is it?

If you’re like most people, you’ll eliminate a few possibilities, narrowing it down to a couple of choices. Then, over time – and along with other factors that may reinforce your decision – you grow more certain that, yes, that penny you’ve chosen is definitely the right one.

But here’s the problem with the story: it’s incomplete. No one mentioned the possibility that the correct version of the penny might not be there at all. That’s one of the problems with the human mind; it wants to pick something, and it’s one of the many problems that can arise from eyewitness identification.

All of the pennies were wrong.

The Importance of "Complete Business Context"

The issues brought to light by the Penny Test translate directly into the world of cybercrime. As the responsibility for cybersecurity moves up the food chain and into the C-Suite, there's an increasing disconnect, which is highlighted by study after study: there's just not enough information.

In the world overflowing with big data, how is it that data is one of the major areas that seems to be lacking?

Simple. There's too much data – and not enough context.

What's the impact of risk to the business? This is the critical piece of information that often gets overlooked.

There is no mutually understood, shared, and high-level language between the IT and the business that allows both sides to really connect, perform critical analysis, make efficient and faster decisions, develop strategies, and, ultimately, work with less friction.

The IT team is often elbows deep in low-level data and investigating red flags, never having a chance to think about or act on a high-level strategy. Meanwhile, executives often don't know what aspects of their company are at risk from mounting cyber threats, let alone where they should allocate resources.

It's as if there's a conversation going on where one side is speaking French, one side Russian, and they're working through an English translator who's using pocket travel guides for both languages.

Mitigating Risk through Cyber Insurance

Cyber insurance is one of the booming categories in the insurance industry. Cyber-attacks are happening more frequently and are getting more coverage by the media, and the costs of those cybercrimes can add up from things like direct financial loss, notification requirements, extra staff hours, legal fees, credit monitoring, fixing vulnerabilities, lost customers and brand damage.

The good news is that cyber insurance policies are beginning to mature.

There are four main types of cyber liability insurance coverage.

1. **Data breach and privacy management coverage** – covers costs associated with managing and recovering from data breaches, including investigation, data subject notification, credit monitoring, and associated legal fees.
2. **Multimedia liability coverage** – covers defacement of websites, media, and intellectual property rights.
3. **Extortion liability coverage** – covers damages incurred from extortion. This could be used in the case of DDoS attacks that demand ransoms, for example.
4. **Network security liability** – covers costs associated with denial-of-service attacks and third-party data theft.

For more information on this topic, read: Using Cyber Insurance and Cyber Data to Limit Your Business Risk

Managing Cyber Risk through a Governance Framework

To overcome this barrier between the cyber world and the business, enterprises need to incorporate a cyber risk governance framework that is molded to their specific needs. While this framework does not require executives to become technologists, it does allow the communication gap to be bridged. Instead of reacting to threats as they hit the organization, cybersecurity to be viewed as part of the overall risk management assessment.

An organization that has a disciplined risk-based approach to cybersecurity threats not only reduces the chance to be victimized, but also provides for a competitive advantage that can be promoted to customers, partners and vendors in the supply chain.

Five key components of a cyber risk governance framework include:

1. **Laying out the responsibilities and management of the myriad of cyber risks that may impact an organization** – Who needs to be involved in making certain decisions and who has accountability for the different realms of implementing a sound cybersecurity program and responding to incidents.

2. **Understanding what cyber trends are occurring in the industry** – This can be accomplished by actively monitoring and assessing the high-level threat landscape.

3. **Comparing cyber trends to the current allocation of resources and budget spent on cybersecurity** – and adjusting as necessary to address relevant risks that the organization faces.

4. **Educating employees, partners and clients on an ongoing basis to instill a culture of cybersecurity** – This must go beyond basic awareness and directly target weak security links – an organization's security or lack thereof goes well beyond its own networks and tools, it is reliant on everyone who touches it including partners, customers and suppliers.

5. **Proactive tests (e.g. Pen-testing) and other exercises/drills to assess for potential cybersecurity weaknesses or gaps in the cyber response plan** – The first time an organization dusts off its security incident-response plan should not be while they're in the midst of a major cyber crisis. Preparation and testing is vital.

Without having a solid understanding of the relevant cyber risks facing an organization, deciding where to focus time, attention and resources can be difficult and may lead to a security strategy that is ineffective and reactionary. By defining a set of key performance indicators (KPIs), executives and boards can empower security teams to better anticipate, manage and mitigate cyber risks. With this power, an organization can turn their cybersecurity practice from a budgetary black hole to a competitive advantage.

So how do corporate leaders become cyber savvy? How do they get up-to-date, continuous information on what might be waiting just around the corner to harm them? More importantly, how do they plan effectively to head it off? The answer is cyber business intelligence.

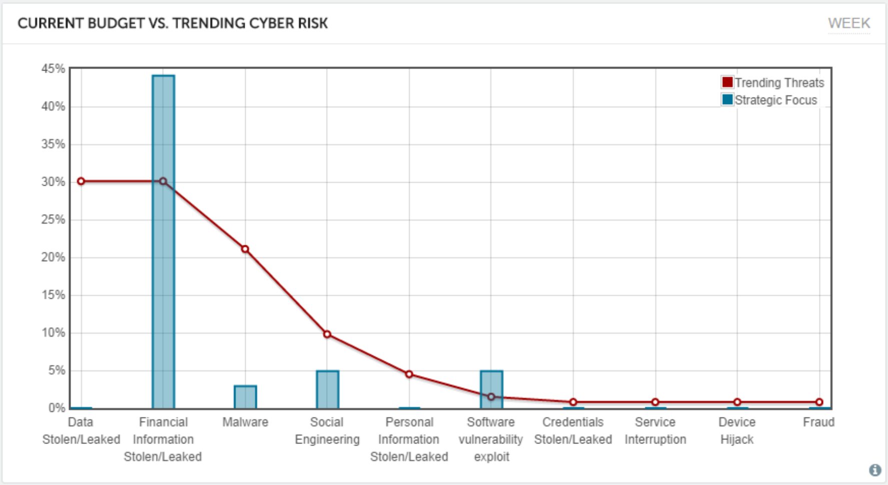
Applying Business Intelligence to Cybersecurity

For all the highly-technical and low-level software and hardware solutions, security tools, people and cyber policies adopted in the market today, no consistent, “right-sized” tool exists at the boardroom level. The problem is that cybersecurity decisions are being made every day without having a complete understanding of what’s going on and what the impact is to the business. While organizations typically look inward at their networks, what’s largely missing is having that high-level awareness of cybercrime data to help answer important questions:

- What are your most crucial cyber assets and what is being done to keep those secure?
- Have there been recent cyber incidents, and if so, have the weak links been addressed?
- What threats are others facing in your sector? What are the most likely internal threats?
- Have any of your partners or those in your supply chain suffered a cyber-attack? Is a policy in place for ensuring those partners achieve a minimum level of cybersecurity?
- Does the organization have a written cybersecurity risk management strategy? Does it include training employees, perhaps the most important line of defense?
- If a breach should occur, who takes the lead? What are the responsibilities of those in the C-Suite and the board?
- What does the company’s cyber insurance policy cover? Is this policy up to date and are the limitations thoroughly understood?

Most businesses use traditional business intelligence as a vital part of their operations to track KPIs – everything from sales performance, customer engagement, brand penetration, and marketing effectiveness to employee retention and financial performance. Business intelligence provides executives and board members with key insights that are used to keep all aspects of their organizations tracking and on target.

Applying a business intelligence approach to cybersecurity can provide this same insights from financial and sales KPIs to the cyber world. Cyber business intelligence can become even more powerful when combined with other, more traditional business intelligence data sets such as budget data. For example, overlaying IT and information security budgets against actual current cyber trends can illuminate coverage gaps, focus problems or overspending.



Screenshot from SurfWatch C-Suite

Conclusion

As the landscape shifts, executives and board members are increasingly forced to take ownership and accountability for any cyber risks facing an organization. No longer is cybersecurity just a technical and operational issue. Cyber issues cannot simply be delegated to the security department; they're issues with serious potential business consequences and they are directly related to corporate governance.

SurfWatch C-Suite is an interactive dashboard application purpose-built to bridge the gap between the technical cybersecurity world and the business side, providing c-level executives and board members with cyber risk intelligence that can be quickly understood and used to minimize the impact of cyber problems.

SurfWatch C-Suite provides significant insights that can be used to steer enterprises to improved risk management related to potential cyber-attacks and their ultimate impacts.

For more information on SurfWatch C-Suite:

- Watch a 2 minute video overview
- Get your free trial today

About SurfWatch Labs

SurfWatch Labs delivers cyber risk intelligence solutions that help organizations understand the potential for cyber-attacks, determine the impact to their business and proactively address threats head on.

SurfWatch Labs was formed in 2013 by former US Government intelligence analysts to go beyond the low-level threat intelligence approach that can drown organizations in data. By aggregating and automatically analyzing vast amounts of data from a wide range of structured and unstructured sources, SurfWatch enables organizations to zero in on their unique cyber risk profile and ensure the most effective risk management strategies are identified and implemented.

With SurfWatch, organizations can immediately understand and act on their cyber risk. SurfWatch Labs: Cyber In Sight. For more information, visit www.surfwatchlabs.com.

Contact us at:

info@surfwatchlabs.com

(866) 855-5444

Follow us at:

f in You Tube g+