Leadership in Cyber Security

Cyber Security: Risk Exposure and Board Interaction

By Sorin Toma

September 2021

Read: 7 – 8 minutes.

PROBABILITY AND IMPACT

KEY TREND:

THE PANDEMIC HAS SHIFTED FOCUS FROM PROBABILITY TO IMPACT

There are some similarities between cyber security and insurance. Probabilities and impact play a major role in determining the level of protection or the premium to be paid up-front.

Let's consider the following scenario.

SCENARIO

What if I said that the probability of a major cyber-attack occurring was 0.1 percent? Would most organizations spend a lot of money to mitigate that risk?

Probably not. I mean the probability is so small (1 in 1000). It won't happen to us. Will it?

What if – instead – I said that the probability of an attack is 1.095 times in 3 years and that time could be tomorrow? And then I said the cost of the impact could be AUD$10 million. That is the same thing in different words and adding information on potential impact.

I'd certainly get more attention and most decision makers would definitely provide the necessary funding to mitigate the risk of such an attack. As long as the cost of mitigating the risk is lower than that of dealing with the impact.

'Framing' the situation to clarify potential likelihood and outcomes, will make a major difference in terms of company boards listening to cyber security professionals.

This will only happen if cyber security professionals talk to boards the right way.

Meaning we need to talk about cyber security risk exposure, or risk profile, risk appetite, and risk tolerance, as well as impact.

KEY INSIGHT

The human brain is not very good at managing probabilities. This has been exposed by the current COVID'19 pandemic. Consequently there is a major swing to repositioning risk from a bias towards probabilities to a bias towards impacts. More importantly the cost of the impact can be identified more precisely than determining the probability of occurrence of an event or incident which can be merely guesswork in many ways.

THE KEY CHALLENGE

CYBER SECURITY IS NOT PERFECT AND IS DYNAMIC MEANING IT IS MORPHING AND EVOLVING

I remember the famous media tycoon Elliot Carver in the movie 'Tomorrow Never Dies'.

"Elliot Carver: Mr. Jones, are we ready to release our new software?

Jones: Yes, sir. As requested, it's full of bugs, which means people will be forced to upgrade for years.

Elliot Carver: Outstanding."

Cue laughter. Sad but in some instances true.

There are many reasons.

- Pressure to get products to market – so compromises are made.
- Highly complex technical environments. Once upon a time the entire technology stack ran on a single machine. Then client-server computing came along. Then smart phones, tablet computers, and the cloud. Now the technology stack spans several layers of communications networks, multiple

PERFECTIONISM IS POSSIBLY A FLAW. IT IS POINTLESS TO DEVELOP A PERFECTLY SAFE SOFTWARE APP IF IT IS UNAFFORDABLE.

machines, the cloud, smart phones and who knows what other devices such as wearables. Cyber security across all of that is a nightmare given the weaknesses embedded in software at every level.

- Law of unintended consequences. Many developers, software engineers and product vendors do their best to make their products secure and the same time easy to use to improve the customer experience and satisfaction. In doing so they create weaknesses that can be exploited by others.
- Deliberately mischievous people searching to profit from product weaknesses or use those weaknesses for other nefarious ends. Hackers. Nation states. Hacktivists.
- Lack of experience and training. Nowadays anyone can produce an App. But is it safe?

And many other reasons. The list is almost endless. But it comes down to one thing and that is human nature which deals with endless compromises and trade-off's every day.

KEY INSIGHT

There is no perfect fully secure product or service. Nothing can protect an organisation successfully 100 percent of the time.

That is why it is important to do the following:

- Everything possible to identify, prevent, mitigate, treat, and/or eliminate cyber security risks by reducing the probability and impact of such an event, to minimize the impact on the business, the cost of resolution, and reputational damage.

Directors and Boards

Boards have many critical responsibilities

- Prepare to deal with a cyber-attack, data breach, privacy violation, and/or any other cyber security event in terms of a robust Incident Management process and policies. Incident Management maturity and readiness must be high.

There are too many important matters pushing into the Board's agenda including regulatory, compliance, audit and risk, social responsibility, diversity, the environment, and many more besides.

Many organizations still do not recognize cyber security as a Board level consideration. Rather security is considered to be a technology matter and is pushed down 2 – 3 layers to technical management level within the organizational structure. That must change, but of course it will take time. Governments have now enacted further legislation to specify board directors' responsibilities in respect of cyber risks.

The funny part is that cyber security is the perfect issue for Boards to consider. Why? Because cyber security is all about risk and all Board Directors understand risk. In fact, many of directors have a legal, commercial and/or risk background.

Still not many companies quantify their cyber security risk exposure in terms of impact for known cyber risks, threat vectors, or events, because the focus in the past was on probabilities not impact.

The most important cyber security responsibilities for board directors include governance, culture (organizational maturity), risk, resilience and compliance.

- GOVERNANCE
- CULTURE
- RISK EXPOSURE
- RESILIENCE
- COMPLIANCE

TECHNOLOGY LESS IMPORTANT

KEY INSIGHT

When addressing boards - talk about risk exposure. Quantify cyber security risk in terms of the cost of impact. Plan and promise tangible, visible, and measurable benefits. Do not focus on the number of attacks prevented. Create the right expectations.

Do not forget the impact of customer and business in terms of disruption, and impacts such as lost sales, lost revenue, and lost customers. Prove the cyber security team's achievements and value to the organisation.

Last but not least protect the reputation of the organisation.

Use examples and case studies to illustrate key points. Many are available – Toll Holdings, Bluescope, BigFooty.com, Marriott, Adobe, Equifax, Canva, Transport for NSW, and many others.

Don't forget the big one – the Nation State Threat.

Remember what is important to protect:

- Customers, Revenue, and Reputation,
- All Staff – Life / Prevent Injury,
- Supply Chain – Prevent Disruption / Fraud
- Assets – Intellectual Property, Data, and Systems / Technology

~~~~~~~~~~~

Prepared by Sorin Toma at Act2Secure Pty Limited
E: Sorin@Act2Secure.com M: +61 419 631 023
~~~~~~~~~~~