Yes! And
Think Innovatively

Involve the Whole Leadership Team to Manage Cyber Security Threats

Jeff Parker & John Brooker

Cyber security involves your whole company *and* your supply chain. Is your company protected from the cyber threat and do you have plans in place to reduce the impact if the worst happens?

The threat of a cyber attack against your business is on the increase. There are many high profile cases involving multi-national corporations where money, data and/or Intellectual Property (IP) have been stolen.

However, there are many more cases involving large and medium sized companies that those companies do not publicise because they fear reputational damage.

What puts you at risk?

Inappropriate Beliefs

Even today, many companies do not have cyber security response plans or appropriate defence measures for their Communications and Information Systems (CIS). Does yours? Some of the reasons for this are that leaders believe:

- Their company is not at risk
- The problem is too expensive to tackle
- The issues are too complex
- They have nothing of value to attract cyber criminals
- It is just a technical threat.

What might be the financial and reputational risks to your company if these beliefs are wrong?

Reliance on Supply Chain

In the global, commercial network where companies of all sizes are digitally connected to facilitate business, **the risk of cyber attack becomes shared.**

If yours is a large organisation that has invested in cyber security, you may still be vulnerable to attack through the supply chain by cyber criminals who target suppliers with a lower level of defence.

If you are the targeted supplier and your company is shown to have been the conduit for an attack against your customers, you risk both the loss of valuable assets to cyber criminals and the loss of one or more valuable contracts with your customer.

> ***"Not only do suppliers risk losing valuable assets to cyber criminals, they also risk losing valuable contracts with large organisations."***

Lack of Knowledge

Like any business risk, the responsibility to ensure a company is suitably protected lies with your Executive team.

However, your existing company contingency plans might not include risk mitigation for the whole company against cyber attacks.

One reason for this is that the technical nature of cyber security means that your business and operationally focused executives may not have the background to assess the risk and business impact of a cyber attack.

Your executives can likely relate to the impact of a fire or flood on their business but would probably struggle to predict the impact of a DNS exfiltration attack.

"DNS exfiltration attack?" Exactly; cyber security is full of technical terminology that does not indicate the business impact it may pose.

You might train all your Executive Team members to become cyber gurus but this seems a little impractical and unreasonable. Consequently, your company may leave cyber security to the IT department or Chief Information Officer (CIO), if you have one.

Equally, it is unreasonable to expect your Head of IT or CIO to know how to provide effective defences for the whole business (and perhaps your customers' businesses).

They will understand the technical risks but may not have the business or operational expertise to identify the business impact associated with these risks.

Therefore, risks and the business impact associated with cyber security should be the collective responsibility of your whole Executive Team and members should understand the cyber threats in a way that allows them to assess all the risks.

> ***"Risks and the business impact associated with cyber security should be the collective responsibility of your whole Executive Team"***

Counter the Threats Through Knowledge

Your company can develop understanding specific to your business by harnessing the collective corporate knowledge of your leaders and key personnel, coupled with subject matter expertise in cyber security to:

- Educate the leaders about the types of cyber security threats, in a non technical way
- Identify the types of attackers and their motivation to attack your business
- Identify the impact of a cyber incident on your business
- Identify the critical business functions that may be at risk, including suppliers
- Identify valuable corporate assets that could attract an attacker
- Determine how your company as a whole will respond if there is a cyber security incident
- Nominate who will be responsible for leading the response to an incident.

To achieve this, consider holding a facilitated meeting with the key people across your company, those with cyber security expertise and possibly with your suppliers; people who really understand the business and can identify the risks and the appropriate responses.

This should be a collaborative, engaging and practical workshop to educate, encourage informed discussion and provide practical outputs.

The output of this collective approach can be aligned to Corporate Governance topics such as:

- Leadership
- Effectiveness
- Accountability
- Remuneration
- Relations with Shareholders
- Institutional Shareholders
- Corporate Responsibility
- Corporate Governance Reporting

Corporate knowledge coupled with appropriate cyber security subject matter expertise enables you to tailor an holistic business response to the cyber threat, which you can embed in your Corporate Governance guidelines.

This planning will provide confidence to your shareholders, customers and employees that the Executive leadership understands and has addressed the cyber security threat.

Most importantly, being prepared may avoid a lot more disruption, protect your reputation and save money too.

"Consider holding a facilitated meeting with the key people across your company"

About the Authors

Jeff Parker

Jeff Parker is a former Vice President of Airbus Group with many years practical experience of working on systems associated with reducing cyber threats. He now uses his CIS, IA and Cyber Security knowledge to support organisations looking for innovative solutions to combat the growing cyber threat.

John Brooker

John Brooker is a former Senior Vice President of Visa and since 2001, he has facilitated workshops with medium and large sized organisations. He helps senior teams to collaborate, engage and think in a more innovative way. He is the author of "Innovate to Learn, Don't Learn to Innovate," available on Amazon.

Our Cyber Leadership Workshops provide you with the necessary cyber and facilitation expertise to develop your plans. Please click here for a brochure or go to our website here:

http://www.yesand.eu/resolve-difficult-challenge/

Contact Us

Write: hi@yesand.eu

Speak: +44 20 8869 9990

Read: www.yesand.eu

Yes! And
Think Innovatively