Cyber Security – doing more with less

Tech Leaders Connect Dinner co-hosted by Norm Cyber

Q1: Where are we going to get the biggest bang for our buck in the cyber security space right now given budget constraints.

Over-investment in IT controls – it s over managed and the business isn t involved as much as it should be

CEOs see it as an IT Problem where it should be a business problem.

Needs to be built in to strategy (business and IT)

Q: Does business know what it should be giving a sh*t about?

- Lack of understanding of what it means for the business

Most businesses should be interested in:

- Revenue
- Operating the business
- Compliance

Need to fit the cyber security in to those areas in order to get traction

Often a large outage can gain significant attention and be sufficient to prioritise business processes and security

- e.g. Bunsfield explosion

Companies have to get lucky every time, a criminal only has to get lucky once.

Tip: Add Cyrillic alphabet to the keyboard of a machine to put hackers off – if they think the user is able to write in Russian, they may well leave the machine alone. FSB are managing many hacker groups targets and who to leave alone.

Cyber security insurance will often want to take control in an incident situation. They have the incident response teams. Don t assume you re on your own.

- Insurance costs will go down if you have cyber essentials plus and/or other security related standards and a decent MS Secure score.

Risk and Issue log is by far the cheapest bang-for-buck

- Need to quantify the risks though.

It must be seen as a cost of doing business..

Develop a process framework where the bigges4t risk/emergency is assessed and what matters 1st – often a good idea for departments to prioritise who s required and what s required in a DR situation.

Also a good win is for architecture diagrams to be up to date.

Q2: People remain without doubt the weakest link in the chain. How do we best help employees improve their personal security when budgets are tight?

Use controls to drive behaviour

Standard training courses very rarely work.

Develop human risk management – just in time nudges when risky behaviour is observed

Demonstrate what good looks like when mistakes are being made

The senior management must be part of what good looks like, they cannot abdicate being an advocate and talisman for the rest of the business

Phishing is still getting more sophisticated and customised depending on the target. Phishing testing is also now enabling a more sophisticated approach to testing the work-force.

- Customising the pseudo attacks to test the company defences is a must nowadays

Senior leaders are more vulnerable to attack. Partly because they re often less secure (they can demand exceptions to standard security protocols) and partly because they have more responsibility and are thus more prized as targets.

- Best way to deal with senior leaders is informal chats and advice/guidance on a one-to-one basis

We have to be make sure that we are able to give a professional opinion to the CEO because it s important that we get this right. It s not a political football.

However, it does depend on how much care there is for the business and the working environment.

Staff need to have the skills to be able to make good decisions on the fly. They need to be empowered to make the right decision. If they think they can allow the tech to do the heavy lifting then they re vulnerable.

IT people often don t get listened to by default, so it s not necessarily the IT team who are the best people to tell the work-force about good practice in cyber security.

The security of the business now has to go in to the home life.

- BYOD appears to be dying due to the complexities of handling the cyber security side of things
- Cheap option: provide everyone with a password manager and a VPN

Q3: How should we develop security, is it possible to outsouce it safely? And the dashboards we re using – do we understand them anyway?

Zero trust networking is misunderstood and cannot be viewed as a panacea for security, but often appears to be considered such.

Need to consider GDPR and PCI along with other compliance requirements. (Audit/Controls).

Secure by design/secure by default is a wonderful catch-phrase, but dev s rarely get it as a concept and don t programme with it in mind.

The Microsoft Secure score is a good conversation starter, but the goal-posts move frequently and it s not clear exactly how to improve the score the whole time.

It s a good idea, if it s affordable to invest in Red Team activities.

Outsourcing of cyber security can feel like we re giving away some crown jewels, but there s lots of suppliers out there that have far more resources and capabilities than we could ever have in the team.

- It feels like having a lynch-pin in the business for security is a good idea (CISO?) and then the rest could be outsourced more safely.
- Responsibility should be internal, but accountability for it can be outsourced.
    - Keep control of strategy, governance and vendor management
    - If you don't then you're a naïve buyer

Often said we shouldn t outsource a problem, so suggestion was to adopt IBM s view of Build -> Operate -> Transfer

Finding the right talent to join can also be hard and perhaps outsourcing can help with that. Any highly talented individual is possibly not going to want to work for an end-user company, more wants to work where there are promotion opportunities and work in a larger team.

- Observation is that new people into industry aren't particularly interested in getting in to cyber security
- Recommendation for developing apprentice type capabilities in the cyber space.

Mistakes are often ignored or glossed over.

- Related to this is the way the aviation handles mistakes vs Doctors. It's highly relatable to what happens in IT and a lack of engagement with really understanding what went wrong.

The report from the British Library is a outlier in that they have been very open about what happened and it s recommended reading.