Cybersecurity Risk Management: What Are You Doing to Reduce the Risk of a Breach?

Modern cyber-attacks can target a wide range of aspects of an organisation, so it's critical to evaluate each aspect of your security program. A strong cybersecurity risk management plan will reduce your risk of a data breach, so make sure you build yours from the ground up.

We've heard a lot about insider threats, such as Sage getting exploited by an employee back in 2016, and about supply chain threats such as NotPetya which was deployed through a malicious software update in 2017.

With so many risk areas to consider it's difficult to feel confident that you've got all areas covered. In this 4 part series, we're breaking security down into the 4 areas we cover during a Cybersecurity Maturity Assessment, offering meaningful advice to address real-world risks.

Under each of the following headings, we look at what helps to build these into robust programs ensuring you are prepared to protect, detect and respond to security threats.

- Cybersecurity Risk Management
- Security Protections
- Incident Detection
- Minimising Impact

What is Risk?

In Part 1 we're talking about "Cybersecurity Risk Management", so it's important to elaborate on what we mean by risk and how it differs to other common terms like vulnerability, threat or asset.

"close the door (vulnerability), to stop the bear (threat), we might get mauled (risk)".

This adage illustrates the idea that you can reduce or remove risk not only by dealing with the vulnerability but also with dealing with the threat and asset (you are the asset). For example, don't live anywhere near bears? Then the risk of getting mauled by a bear isn't a problem. Not in the cabin at the time? Then the getting mauled by the bear isn't a problem.

When it comes to risks you have several options with how to deal with them: fix, mitigate, or offset. In the context of information security, a fix could be updating an outdated piece of software. Mitigating a risk could be a compensating control such as a web application firewall, which doesn't fix the vulnerability directly but makes exploitation more difficult or

no longer possible. Offsetting could be transferring the risk to someone else, such as contractually passing it on to a supplier or insurance provider.

Here we take a look at what to consider when managing risk within your organisation.

Build a Security Policy

One of the difficulties with security is simply "where do we start?" A sensible place to begin when thinking about risk management is to define your risk appetite. As it's often impossible to completely remove all risk, you need to reduce risk to the point that it's acceptable to the organisation.

A security policy is a document defining how a company plans to protect it's assets. It will outline what level of risk you're willing to accept and how you grade those risks. If your security policy says to mitigate all issues above a "medium risk" without defining what denotes a medium risk, it's useless.

Promote a Security Culture

It's essential for modern companies to find a way to demonstrate to staff that security is critically important to the organisation, encouraging users to ensure they take security seriously each day. Helping staff members understand security issues and how to report them are the first steps to building a security culture.

An important factor of promoting a security culture is also removing blame. The NCSC has talked about this previously when dealing with phishing:

"Many organisations believed that if users were blamed or punished for clicking phishing emails, they would somehow be able to spot them next time around. Quite simply, this does not work, and it can also cause a great deal of distress and even distrust between users and security."

If a staff members tells the IT team they've fallen for a phishing scam and they are blamed or punished, they're not going to end up more likely to spot the next phishing email – they're just going to end up less likely to tell the IT department they fell for it.

Encourage Board Involvement

Getting board buy-in into security is critical; there's no point in pushing security throughout the company if the CEO is using 'Password123' for his email. However for some organisations, getting the board to take security restrictions seriously, to enforce policy from the highest level and to be included in discussions about what happens in the event of a breach can prove difficult.

The NCSC have created a board toolkit to encourage discussions about cybersecurity to take place between the board and their technical experts. This toolkit includes the information the board needs in order to make informed decisions, allowing them to evaluate and prioritise risks, and take steps to manage them.

Whilst the technical team might have technical insight that the board don't have, the board might have business insight that the technical team don't have, so it's important to remember that you're on the same team. Developing communications in a language both can understand is critical.

Access Your Supply Chain Risk

Security risk considerations should not be limited to your internal systems. Most organisation use suppliers to deliver products, systems, and services such as hosting providers, software solutions and apps. These supply chains are often large and complex, therefore asking your suppliers the correct questions to determine who owns that risk and what the penalties are if that risk isn't properly addressed, is critical. Never assume a third party has it covered!

Offer Security Training

When we talk about security training, we aren't just referring to security awareness training for the wider business, such as teaching employees how to report security threats or understanding the importance of passwords and two-factor authentication. Your security and IT teams also to need to be up to date with the latest threats and how to deal with them. If you're not prepared to budget for certifications and courses, they're unlikely to be learning everything they'll need to keep your systems safe. Do however, check that the training is fit for purpose. It needs to cover the threats that your organisation face as well as the protections that you have in place.

It's also recommend to ask staff for feedback following training and encouraging them to highlight any areas that they don't feel were adequately covered so that training in the future can be improved.

Introduce Security Roles

It is advised to determine who in your organisation is responsible for security, at each level. Who is in charge of tracking security work, raising threat intelligence items to the board and pushing for discussion on security matters? Each organisation is different. Maybe you have a Security Manager, or a Chief Information Security Officer, or maybe it's the responsibility of your Chief Information Officer – as long as you have an individual responsible for driving those discussions.

You should also have somebody at each organisational level who is responsible for escalating security issues that are discovered, ensuring there's no disconnect between your staff and the person who is overall responsible. Consider delegating a certain amount of security responsibility to each of these people to ensure that the escalation of matters doesn't swamp the CISO with issues, but clearly defines what is delegated and to what degree.

Reviewing your Risk Management Strategy

At Secarma we believe that all businesses, regardless of size are required to develop a thorough understanding of the risks they face and be given direction by a trusted advisor to improve their own cybersecurity maturity.

With this in mind we have developed a Cybersecurity Maturity Assessment (CSMA), a simplified version of the NCSC Cyber Assessment Framework, which covers all the areas discussed in this blog and following blogs in this 4 part series.

Download our CSMA information pack to find out more about how we can help you assess and improve your current security program.