10 things every board should be doing about cyber security - guest commentary by NZRS CEO

May 2016

Introduction

This article is by Jay Daley, Chief Executive at NZRS Limited, a wholly-owned subsidiary of InternetNZ. NZRS is the registry for .nz domain names and the operator of the .nz domain name space.InternetNZ. With such a central role on the internet, cybersecurity is a key issue for NZRS.

Jay's article first appeared on the NZRS blog.

Read more here.

The Detail

After many years with cyber security as a fringe issue, more and more boards are becoming aware of just how important it is that they have a clear oversight of the company's cyber security posture and the risks to the company if they don't. For boards still grappling with this complex area I share these 10 hard learnt lessons to help them develop that clarity.

1. Pay experts to try and break in – it's the only authoritative way to tell if your company is secure.

Risk analysis, well designed processes, regular process audits and intrusion detection tools are all necessary parts of good cyber security but it's not good enough to rely on those alone. The one method that absolutely has to be utilised if you want peace of mind is paying experts to try and break into your company, the service known as penetration testing. If experts using the same tools and techniques that cyber criminals have at their disposal can't break in, then you have the strongest assurance it's possible to get that your company is safe.

What you're quite likely to find though, is that they can actually break in and possibly quite easily. Reading a report from penetration testers for the first time that explains just how easily your company defences were breached is sobering to say the least. That first shock is slightly tempered when the executive explain how quickly they have acted to bolt the stable doors, as they inevitably will have given the wake up call a report like this delivers. But when the second or third penetration test fails to find a way into the company that quiet panic is finally replaced with a reassuring sense of security based on the strong evidence that penetration testing delivers. No amount of passive audit can deliver this surety.

2. Rotate security auditors every few years and look for skills not badges.

There's a natural progression in every industry that sees pioneers in the industry organise to develop a capability maturity model and issue accreditation based on assessment against that model. By the time an industry has been around for a hundred years or so the whole industry is involved and the process of accreditation is

comprehensive, consistent and robust, and so can be taken as a trusted sign of quality.

The cyber security industry isn't that mature yet and while the service provided by an accredited auditor can be excellent it is not going to be comprehensive as the field is just too broad for one firm to cover it all. In financial audit, rotating the lead audit partner is sufficient as it ensures a fresh set of eyes, but for cyber security a fresh set of eyes is not enough. Instead it needs a whole new audit company with different methodology, people and tools to tackle things in a different way and thereby build up that comprehensive coverage.

3. It's not just loners in their bedrooms that you need to protect against, it's organised criminals with automated hacking tools

The loners in their bedrooms are still there and still a threat but things have developed a long way since a kid hacking networks just for the thrill of it was the biggest threat you faced. The criminals have moved in and there are organised gangs out there who hack into companies for a variety of reasons. Some steal money, some steal company information they can sell, some are paid to disrupt a company by a competitor, some disrupt companies for a blackmail payoff and some are a mix of hackers and activists - hacktivists.

These organised gangs don't have to be particularly technical or innovative as there's plenty of software out there that automates almost every step in the hacking process, from target identification to vulnerability assessment through to the actual process of taking control of a company's computers. Some of these tools are highly sophisticated and criminals can pay a high price for them; a commonplace investment given the potential for profit these tools provide.

To add to the complexity there are a few countries with state sponsored hacking teams that act indistinguishably from criminal gangs. They have the same modus operandi but economic or political espionage as their primary objective. Unlike criminals motivated by profit, these teams are protected by legal impunity, have far greater resources at their disposal and are much more technical.

4. If your government offers to help, then take the offer seriously.

The number of clever hackers out there looking for new vulnerabilities and developing new means of illicit entry are far fewer than it would appear given the volume of hacking attempts. As I noted earlier, the reason there is so much active hacking taking place globally is because the tools have become so powerful and so simple to use that it doesn't take much knowledge to use them.

Increasingly, and particularly in certain countries, the clever hackers who invent the techniques used in these tools are being recruited into military cyberwarfare teams as the militarisation of cyberspace accelerates. The net result is more and more successful intrusions being pinned on foreign state-sponsored hackers using their own home grown and initially undetectable tools. Worryingly, the list of probable victims covers a wide range of companies and industries and there is no guarantee that a smaller company is not important enough to be a target.

To counter these threats, governments have developed expertise to defend themselves and built networks for information exchange with allies and trusted third parties. If your government offers that expertise to you then at the very least it is wise to run a trial to see what they can identify that your vendors have missed.

5. Ask for the same visibility of cyber attacks on your employees as you have for your IT systems.

There's an entire branch of hacking, called social engineering, which deals with tricking people into breaching their own cyber security. The latest development to make the headlines is the whaling email – an email that pretends to come from the CEO or other senior manager, instructing the finance team to make a payment, which uses subtle psychology to bypasses the normal authorisation processes.

Boards expect to see documented risks and mitigations of attacks against IT systems and this expectation should be the same for social engineering attacks as they have a different threat profile and require different mitigations.

6. All of the staff in the company, from top to bottom, need to be trained to detect cyber attacks.

The safest approach to cyber security training is to mirror the approach you take to health and safety and treat it as a company wide problem that everyone has to understand and play their part in. Any staff that are not trained are oblivious to the risk and that leaves the company vulnerable to a step-by-step attack getting its first foothold with an untrained member of staff.

Staff training in this area, which could be as simple as two-hour workshop, aims to do two things. The first is to help staff identify potential attacks by showing them a wide variety of historic and current attacks. This is vital because most employees who don't work in IT simply have no idea what to look out for.

The second, even more important aim, is to help employees understand how these attacks work and how even someone junior in a company may be carefully and individually targeted as a stepping stone to a bigger target. Once that understanding is embedded throughout the company the chances of falling victim to even a new and innovative attack are significantly diminished.

7. Ensure that third parties who discover vulnerabilities into company systems have a safe way to report them to the company.

Vulnerabilities in company systems are going to be discovered by third parties on a regular basis and boards have a choice on the strategic response to that. Some companies operate on the belief that if information on vulnerabilities can be suppressed from getting into the public domain then that will keep them safe. As a result, they respond with legal action against anyone who even discloses they've found a vulnerability let alone shares the details.

While this can provide short-term protection for a company's reputation it doesn't stop people looking for vulnerabilities (or finding them), it doesn't stop that information being sold to criminals and then exploited, nor does it protect the company's reputation in the longer term when one of those vulnerabilities leads to a hack too large to keep secret.

The forward thinking approach is to publish a Vulnerability Disclosure Policy that tells third parties exactly how to tell the company about vulnerabilities they find without the risk of legal action and ensures the company has time to fix them before any public disclosure. It's not uncommon for the discoverer of a vulnerability to use it against the company out of sheer frustration if they feel they can't report it safely or are not listened to.

A particularly enlightened approach, pioneered by the likes of Google and Facebook, is to pay people who discover serious vulnerabilities and follow the rules when reporting those. Even a small company can do this, paying out in the 10s or 100s of dollars at most.

8. Ensure that the company has a clear policy to guide how it responds to a major customer data breach

There's a familiar pattern emerging where companies that are hacked are accused of taking too long to admit the hack (appearing only to do so when they have no choice), seeming to underplay the scale of the hack, and apparently refusing to acknowledge that they could have done things better. The overall impression is of companies that abandon their stated values when things get hard.

The problem starts when a company does not accept that once breached it is no longer in control of events. There are some types of hackers namely hacktivists and hackers for hire, who want the full extent of the breach known and will deliberately embarrass any company that tries to bury the news. Then there are the affected customers who will known soon enough if their data is stolen and exploited, plenty of whom will make a public fuss.

The risk of falling into this trap can be minimised by a clear policy that sets out what's important for the company and what customers can expect the company to do. In other words, a reminder to uphold the company values however bad the breach.

9. Upskilling the board in cyber security should be a top level board priority.

The jargon can be baffling and many of the concepts are new and unusual but boards have to push through that and upskill as the risk from cyber security is too high to be left to the executive. At a minimum your board (or a committee) should be comfortable in receiving a specific cyber security risk analysis and specific cyber security audit reports. Ideally, around the board table there is sufficient knowledge of the concepts to scrutinise the company approach to cyber security as deeply as you scrutinise other areas of high risk.

Take encryption for example. Many companies that have been breached could have prevented the loss of critical data by encrypting that data. That would have meant that the hackers that broke into the systems would only have been able to steal a file of garbled nonsense. Those companies needed a board that scrutinised their cyber security enough to have asked the question "but what if they do break in?".

10. As board directors, take your personal IT security very seriously.

Managing your own IT as a board director sitting on multiple boards each with its own IT systems and processes, can be complex. In particular, using multiple email systems and multiple devices just reduces your productivity and so there's a tendency to try and short circuit some of that by using a personal email address and personal laptop/ tablet. Being a board director of course, you're more likely to ensure that the policies allow this and are less rigid for the board than for staff.

What should be obvious to every board director by now is that you are some of the highest value targets in the company. While it's unlikely that as a director you'll have any privileged access to IT systems, what you do have is authority both explicit and implicit, and that's what the hackers will target and try to hijack. A hacked email account can be used to great effect by a skilful hacker. They know what psychological techniques to use to pressure someone receiving an email they think comes from a board director, into bypassing the ordinary internal controls.

It's therefore vital that board directors take the security of their personal IT very seriously, which means including it in the company's security audit plans as a recognised high risk target.

That's the top 10 and I hope that's inspired you, or even scared you, to implement them. If your board implements just half of

them, you'll probably be in the top 5% of cyber security aware companies.

For further reading try the excellent IoD Cyber-risk practice guide.

(This article first appeared on our normally quite technical company blog).

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com