KPMG
cutting through complexity

Non-Executive Director's Update
Cyber Security Breaches

Many Irish companies believe that they can protect their IT systems and data by investing in anti-virus software and other IT security solutions and products. However, cyber criminals are becoming more sophisticated in their attacks and are targeting companies using a number of different methods and strategies.

Information regularly ends up online through negligence, deficient document publishing procedures, or as a result of earlier security breaches, and is useful to hackers as it helps profile the target firm's IT and employees. Information which may inadvertently be made available through an organisation's website, but can be leveraged by cyber criminals, includes employee contact names and email address, IT system and software versions and security policies indicating the types of security mechanisms in place to protect IT systems and data.

Non executive directors can play a role in addressing this risk. Firstly, a review of what information your organisation may be leaking can be performed. Partner businesses and third-party suppliers must form part of this review. As enterprise security programs get more robust, it's easier for attackers to access a trusted neighbour's network, which may have more security deficiencies.

Over a six month period, we performed research in this domain focussing on the Forbes 2,000. The aim of this research was to perform the same initial steps that cyber attackers and organised criminals execute when profiling a target organisation for attack. All information was sourced from the public documents located on their corporate websites, document meta-data, search engines and public internet forums, and no hacking or illegal actions were performed.

Vulnerable web servers

Corporate websites are supported by a number of web technologies and when a website is accessed, the web server often reveals its software version which is typically hidden from a web browser's view. Such information can prove to be of significant value to an attacker when profiling a remote target site and server.

We found that 16% of Forbes 2,000 corporate web servers are vulnerable to cyber attack due to missing security updates or outdated software.

Sensitive information leaked within meta-data

Document meta-data is information 'about' a document, or information on its properties. It often specifies who created a document and when or where it was created. This information can provide cyber criminals with a very useful view of a target organisation's IT environment including usernames, email addresses, software versions and information on the internal IT network. We found that 78% of Forbes 2,000 corporate websites leak some form of potentially useful information through document meta-data.

Online forums, chat rooms and newsgroups

Cyber attackers will spend time trawling through online forums, message boards and newsgroups for information relating to potential targets. By participating in online IT related discussion boards and special interest groups, cyber criminals can garner very useful information about different organisations IT applications, systems and network which can be used to identify vulnerabilities which can be exploited.

During our research it was found that companies involved in technology and software post far more information to online forums and newsgroups than all other sectors combined.

How to minimise your exposure

Non executive directors and senior executives need to continuously review and challenge what you are being told by your teams about information security and cyber defences. Just as cyber attacks have evolved, companies must evolve by re-evaluating their own ability to detect, defend and respond to cyber-attacks.

Companies need to establish what controls are in place and how these are being tested to ensure that they are sufficiently protecting the organisations IT systems and data.

Practical steps can be taken to improve cyber security through reducing the amount of data which companies expose on the internet. First, an assessment of what an organisation and its suppliers currently leak can be conducted. Then, where possible, meta-data can be cleansed from existing published documents and steps taken to ensure all corporate devices are protected through the application of relevant security updates. In addition, an important proactive measure is to ensure that all employees understand the value and sensitivity of the information they possess and, more importantly, how to protect it. This behavioural change can be supported by policy changes aimed at minimising unintentional or undesired corporate information appearing on the internet, either directly or through suppliers.

Contact us

David Meagher
Partner
T: + 353 1 410 1847
E: david.meagher@kpmg.ie

Michael Daughton
Partner
T: + 353 1 410 2965
E: michael.daughton@kpmg.ie

Niall Lavery
Associate Director
T: + 353 1 410 1433
E: niall.lavery@kpmg.ie

kpmg.ie/cyber

Produced by: KPMG's Creative Services. Publication Date: June 2015. (874)

Questions to ask your Board

How can Board members get on top of this issue?

- Does my organisation meets all of its obligations for information assurance?
- Is data secure in my organisation?
- Do we fully understand our current vulnerabilities?
- Do any of our supply chain partners put us at risk?
- Do we meet the information security requirements to bid for government contracts?
- Are our competitors ahead of us? If so, does this give them an advantage?
- Who in our organisation is responsible for cyber security issues?
- How can the Board become more proactive, focussed and preventative?
- How do we move from reacting to, to anticipating cyber-attacks?
- How do we make sense of the cyber threats we face?
- How do we demonstrate the return on investment of our cyber security measures?
- When was the cyber threat last examined by the Board?
- Is cyber part of the Board's strategy discussions?
- Does our CIO know when to act? Which tactical option to pursue? Has it been effective?

Does your Management team know what to do if your organisation is attacked?

- What should our response be?
- How effective has our response been?
- What do you know about the people/organisations responsible for the attacks and how do they operate?
- Are there any patterns regarding cyber-attacks that make our information and assets more vulnerable at certain times?
- Who should we be sharing threat intelligence with and how?

What can the Board do about it?

We believe in five principles that can help organisations manage the cyber threat proactively and help reduce the risk to customers, shareholders and employees. These are:

1 **Prepare** - understand and improve the current state of preparedness against cyber-attack.
2 **Protect** - design and implement a cyber-defence infrastructure.
3 **Detect** - respond and investigate cyber-attacks.
4 **Integrate** - embed cyber security in the culture and decision making to help ensure it stays one step ahead.
5 **Transformation** - organise and deliver a wholesale program of change to improve an organisation's cyber security.

Cyber Maturity Assessment (CMA) provides an in-depth review of an organisation's ability to protect its information assets and its preparedness against cyber-attack.

Please contact us for more details.