www.pwc.ch/cybersecurity

Ransomware

Why is the latest attack different and what is its relevance for boards?

pwc

A large number of organisations across a range of industries have been affected by the recent WannaCry ransomware attack

What steps should I take?

There are many pragmatic steps that an organisation can take to reduce the likelihood of cyber security incidents, limit the impact when one does occur, and to recover swiftly and effectively. There are four key areas where we advise organisations to focus their efforts:

Robust business continuity planning and exercising: ensure individual user systems and key servers can be restored rapidly from backups, and that the frequency of backups aligns to the time-frame of data your organisation is prepared to lose in the event of any system being rendered unusable.

Crisis and incident response planning and exercising: ensure your team is well-versed in a quick reaction to ransomware events and in restoring services.

Strong security hygience policies and user awareness: prevent ransomware entering your IT environment in the first place, by enforcing strong controls at email gateways and network perimeters, and have robust awareness campaigns for employees.

Rigorous patch and vulnerability management: reduce the likelihood you will be exploited with a robust programme to manage your vulnerabilities.

Threat Intelligence and detection: improve your detection, identification, response and recover capabilities with Threat Intelligence and stay ahead of the current threats affecting your company. PwC Intelligence services provide actionable intelligence in the form of reports, briefings and alerts on the cyber threats targeting your industry sector and more precisely your organisation. Additional reports on specific topics (e.g. malware campaign, techniques and tactics used by threat actors) can be requested. PwC also offers engaging security awareness raising sessions and training.

What if I've been affected?

PwC never recommends paying in response to a ransomware – unless there is a threat to life. Doing so fuels the ransomware economy, funding development of additional ransomware techniques and campaigns.

Please get in touch with a PwC team member listed overleaf or email: cyberinvestigation@ch.pwc.com

Relevance at Board Level

Cyberattacks are not just a technology or IT issue but have significant impact on the business and are more and more threatening the core of an enterprise. As a result boards request often support in regard to preparedness but also in how to deal with cyber incidents as the technically focused incident response activities more often than not fail at bringing the relevant topics to an appropriate level so that boards can base their decisions and communications on a relevant understanding. Sometimes it is also appropriate to have an independent verification of the technical activities in regard to approach, scope and performance to protect the interests and obligations of board members.

What are the risks going forward?

Even after a highly visible attack such as WannaCry and the recognition that this was most likely only the first of many larger waves of such attacks, companies must not forget that ransomware is just one threat among a myriad of others. Sophisticated espionage campaigns leveraging third-party providers, professionally tailored phishing e-mails, artful banking malware, increasingly stronger DDoS attacks and cunning social engineering schemes pose a serious threat to Swiss and international companies across all sectors. These threats are fueled by the wide commercialisation of hacking tools and services on the underground markets of the dark web that makes such attacks accessible even to lay persons, as well as by the growing attention state actors give to the cyber sphere. The WannaCry worldwide campaign has reminded once again that no sector is immune to cyberthreats and that most companies need to significantly catch up on their preparedness.

Seven principles for governance of cyber security risk

A comprehensive and practical approach is needed to better manage cyber security risk. We have developed seven principles to help organisations structure their governance of cyber security risk. Adopting these practical steps will help boards and management debate and make the tough decisions needed to develop an adequate response to the threats they face.

1. Real understanding of exposure

Many organisations fail to understand properly why they might be targeted; what might make them vulnerable, and how a successful attack might impact them.

The understanding needs to extend beyond the enterprise. It must reflect relationships that could make them a target and the complexity of digital connections that could cause them to be vulnerable: suppliers, service providers, partners, cloud services, critical data feeds, staff and customers to name a few. It must also reflect what data the organisation manages, why and where.

Building this understanding, and ensuring it stays current, is critical to ensuring that the response to the risk is adequate.

2. Appropriate capability and resource

Effective cyber security requires capable skilled resource that is empowered and resourced to shape an organisation to be secure. Boards need to be confident in the capability of their security function and its leadership, their ability to drive a broad response to cyber security across the whole enterprise, and rapid access to wider capability when required. Effective executive ownership is critical, with the CEO taking an active role.

For boards to be effective in this area, they themselves require sufficient capability to probe, challenge and support management. Board-level time needs to be devoted to drilling into detail, since that is where significant issues can lie. Capable non-executives are required, potentially supported by a board sub-committee with additional expertise.

3. Holistic framework and approach

A holistic approach to managing cyber security needs to not just build and operate effective cyber security controls. It must also reduce the complexity of the technology and data estate to which those controls are applied (inside and outside the organisation); address process and cultural/human vulnerabilities that attackers are increasingly targeting, and embed cyber security consideration in all business decision making.

Process vulnerabilities are often overlooked, but common targets. Examples include weak registration processes to online services or distributing sensitive data to an inappropriate third party for processing. A simple, but often exploited human vulnerability is poor password management, such as reuse of credentials across applications.

Recognised frameworks, such as those published by the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) can help define required cyber security controls, but taking a broader approach is critical. Meaningful measurement is crucial, not just of controls but also extent of exposure.

4. Independent review and test

As with other significant issues, boards require independent validation and testing of their believed cyber security posture. This is achievable through independent expert review of cyber security frameworks and approaches, and even certifications of specific elements.

Strength of individual critical controls and systems needs to be tested and techniques such as 'red team testing' by skilled penetration testers can assess effectiveness of overall response to specific likely attack techniques (but only at a point in time). The speed with which issues identified through independent review and test are resolved should be measured.

5. Incident preparedness and track record

Cyber security incidents are inevitable. Governance of cyber security risk is important but effective governance when the risk materialises is critical.

Ensuring that focussed, practiced plans exist to respond to, and recover from, the most likely scenarios is essential. These need to consider not just technical resolution, but also business management, reputation management and management of legal and regulatory risk. Incidents need to be tracked, accurately reported, and lessons learnt.

In addition, organisations need to be able to respond appropriately to the reporting of vulnerabilities that could make products, services or internal processes vulnerable to attack.

The approach to incidents and vulnerabilities needs to be considered through suppliers and service providers, and not just within the 'perimeter' of the organisation itself. Exercising response at all levels is crucial, including the executive committee and board.

6. Considered approach to legal and regulatory environment

Cyber security cuts across an increasingly complex legal and regulatory environment globally. Industry regulation, data protection regimes, national security legislation, reporting requirements and product liability are a few examples of legal and regulatory environments that need to be understood, and a considered global response developed and maintained.

7. Active community contribution

No organisation can protect itself in isolation. Attackers commonly breach one organisation in order to target another, and replicate successful attack techniques rapidly. Thus collaboration is essential: between organisations within industries; through supply chains; between public and private sectors; between companies and law enforcement/intelligence agencies, and even with customers.

For more information on this Ransomware attack, please see our website at pwc.ch/cybersecurity

Reto Häni
Partner and Leader Cybersecurity
+41 58 792 75 12
reto.haeni@ch.pwc.com

Yan Borboën
Partner Assurance
+41 58 792 84 59
yan.borboen@ch.pwc.com

We have done this before

PwC offers a truly global cyber security service, with over 3,200 professionals across the globe, enabling us to use a global network and deliver value locally or wherever you are operating from.

Our full range of services includes technical, business and legal expertise to help you navigate the challenges and threats faced by business today at technical as well as at board level.