Cybercrime: Top protection tips

By Harsha Gordhan

30 Mar 2015

Cybercrime is generally defined as any form of criminal activity involving the use of computers and the internet. According to the McAfee Report titled Net Losses: Estimating the Global Cost of Cybercrime (June 2014), cyber-crime equates to 0.14% of our GDP - that's' a staggering R5.8 billion.

Harsha Gordhan

According to the respondents of PwC's Global Economic Crime Survey (2014), 50% of respondents stated that they had been victims of economic crime. The industries most at risk are financial services and retail and communication; however this spans 18 industries including automotive and manufacturing. Amongst the most commonly reported types of economic crime, cyber-crime affected 26% of respondents in South Africa.

South Africa has been victim of a few major cyber-crimes that stand out. The SA Post Office financial institution Postbank was target of a cybercrime syndicate that stole R42 million from over the New Year holidays in 2011. The incident occurred three years after Postbank spent over R15 million to upgrade its fraud-detection service.

Junaid Amra, a senior manager of PwC who assists clients and law-enforcement agencies with cyber-crime investigations and IT security provides a set of seven baseline requirements that every organisation should consider implementing in order to protect itself against being a victim of cyber-crime. Amra commented that he sees these as the bare minimum and organisations may find additional safeguards that need to be implemented as an organisation matures and new threats emerge.

- **IT governance**: IT governance, in essence, is the framework that guides the management of the IT environment. This translates into having policies and procedures that guide the IT department in various aspects, including setting up security within IT environments. Amra stated that: "In my experience, the majority of organisations that have suffered breaches did not have the appropriate level of governance embedded within the organisation."

- **User security-awareness training**: Organisations are spending millions on IT security; however the weakest link is often employees. Employees need to be educated about good security practices and need to be made constantly aware of the latest trends from a security perspective. As an example, one of the common ways of breaching networks is by sending emails with malicious software attached. Once the attachment is opened, it can compromise the computer allowing an attacker full access to the information and resources that the particular computer has access to. Continuous training will empower users to identify these. "Fraudsters use current events to trick users into opening documents containing malicious software. For example, during the last FIFA World Cup, fraudsters sent out emails offering free World Cup tickets if people clicked on a link contained in the email. Once the link was clicked on, users were taken to a compromised website that downloaded malicious software targeting bank account information," said Amra. He further stated that similar scams are evident on social media, which users need to be aware of.

- **Monitoring controls**: Based on current trends, Amra noted that attackers are able to breach networks and have access for extended periods of time without being detected. In some cases this period has been longer than a year. What this means is that security monitoring processes are ineffective. Unfortunately, many organisations are simply doing this to satisfy audit or compliance requirements. Setting up an effective monitoring process involves proactively engaging with risk managers to understand what the business risks are and what information will be required in the event of an incident. Once this is defined, the IT solutions can be enabled to log this information and, more importantly, the logs need to be critically reviewed on a regular basis for the process to be effective. All data should be backed up and encrypted. It should also be stored offsite in the case of a burglary or fire.

- **Controlling third-party access**: Third-party vendors with extensive access to networks, which are often not monitored, controlled or involve access that is not revoked once the third party has completed its tasks. These accounts are compromised and attackers can, depending on the situation, gain remote access to a network through these accounts. A good process would entail that third-party access is revoked each time a task is completed and granted again when required. In addition, the level of access provided to the vendor should be appropriate to the task at hand.

- **Patching of systems**: Patches for systems are released by software vendors in response to vulnerabilities detected on their systems. Hackers and other malicious individuals in some instances reverse engineer patches to understand what a software vendor is trying to protect against. "This means that if you have not applied the relevant security patches, your systems and networks are exposed," warned Amra. Whilst this might seem like a simple task, a large percentage of successful attacks are due to organisations not applying the relevant patches to systems and user workstations.

- **Anti-virus and anti-malware protection**: "There's no question as to whether you require this or not," said Amra. Most, if not all, organisations have deployed solutions in respect of anti-virus and anti-malware protection. "Again, through the reviews that we have performed we find that organisations are not updating the software with the latest virus and malware definitions quickly enough. As a result they will not be protected against those particular strains of attacks," stated Amra. Amra continued to say that, in a number of instances, he has found that anti-virus and anti-malware software has been misconfigured. This could allow users to bypass the security software or exclude the scanning of devices like flash drives or DVDs.

- **The changing face of IT security**: Amra commented that the nature of IT security has changed significantly over the last decade and medium to larger organisations require an IT security officer or someone dedicated to assist with ensuring that security measures are deployed, monitored and, more importantly, configured to protect the organisation.

The PwC Global State of Information Security Survey (2015), notes that businesses need to evolve from simple security to cyber risk management that is in line with the changing landscape of cyber-crime. It is not a one-off approach. The Protection of the Personal Information (POPI) Act dictates how organisations handle personal information and determines how an organisation protects the personal data it has. Should personal information leak, companies risk incurring large fines for breaching the Act.

Implementing these vital security steps within your organisation will help make your business a less attractive target to a hacker. Businesses should also consider purchasing a cyber-insurance policy that will provide protection if a hacker is

successful in stealing your data. With the rise of internet connectivity in Africa, protecting one's business against cyber-crime should be at the forefront of everyone's agenda, as investing in protection now, could avoid potential costs in the future.

ABOUT THE AUTHOR

Harsha Gordhan has a passion for people - she has worked in consumer market research for five years linking consumers and brands. Yet the one thing she may love more than people is words. When she isn't covering weddings stories for *The Sunday Times*, she's out and about enjoying the vibrant city of Johannesburg.