THE FIGHT IS ON

The true cost of cybercrime to business

By Corien Vermaak,
Cyber Security Specialist
at Cisco Systems (South Africa)

In 2019, it was reported that cybercrime breaches were up 11 percent year-on-year, and had increased by over 67 percent over the past five years, according to Accenture's global Ninth Annual Cost of Cybercrime Study.

Some countries are seeing alarmingly high increases in numbers, with the US, Germany and China leading the cost of cybercrime list. According to the South African Banking Risk Information Centre (SABRIC), South Africa is also at greater risk, seeing an increase of over 100 percent in mobile banking application fraud alone.

According to the Australian government's 'Stay Smart Online' initiative, 50 percent of incidents can be blamed on web-based and insider attacks. This concurs with the annual IBM X-Force Threat Intelligence Index 2018, which concludes that 'inadvertent insiders' accounted for two-thirds of all the records that were compromised. Our workforce is also one of the largest contributors to damages suffered during attacks, as the loss of productivity is mostly understated. According to the Cisco CISO Benchmark Report, user awareness is a critical focus for Chief Information Security Officers (CISOs) globally.

A ransomware attack takes place every 14 seconds, and it's estimated that this will increase to a rate of every 11 seconds in the next two years. And the largest target sector? According to three different reports, it's the small business. The Australian government states that 60 percent of targeted attacks strike small and medium businesses. On average across all the research, more than 50 percent of attacks are focused on the smaller business.

Corien Vermaak, Cyber Security Specialist at Cisco Systems (South Africa)

Looking at the the enterprise level, however, it is clear that the financial sector is mostly affected. According to a Ponemon Institute report published by Accenture, the financial sector suffers the greatest losses per breach in terms of costs.

If we look at the actual cost per breach, the jury is still out on this discussion. However, the industry is in a position to roughly quantify what these breaches are costing organisations.

11%
Year-on-year increase in breaches

> 100%
Increase in South African mobile banking application fraud

50%
Incidents are blamed on web-based and insider attacks

2/3
Of all compromised records are due to 'inadvertent insiders'

Considering figures reported by SABRIC, the South African financial sector places the costs at $1,2 million per breach. The Australian government reports that, according to reported cybercrime research, an attack amounts to in excess of $270,000. Germany is reported to be within the top three in terms of what cybercrime is costing countries as a whole, with $50 billion in losses.

These numbers are thought-provoking, but let's simplify the matter of cost further. Based on several reports, one of the most prevalent attack vectors is web-based compromise, and all of the reports and research teams make a noble attempt to quantify some of these breached in a statistically relevant way.

It is reported that the cost per web-based breach varies between $53,000 up to $114,000, equating to an average of $83,000. If you take into consideration that 60 percent of attacks are focused on the SME sector, this figure is alarming, begging the question of whether a small or medium business can survive an attack at that cost?

On the issue of how much attacks can set us back, it would be irresponsible not to mention the added risk of regulatory fines. Even though all the reports mentioned how the cost per attack is calculated – including business interruption, information loss, revenue loss and equipment damage, among other factors – most attacks target data. If a company is found to have not done what is reasonably expected to protect its data, these attacks could also be subject to fines by data privacy regulators.

Taking this this one step further, as in the case of Equifax, the cost of a breach could be affected by civil procedure or corrective actions required to assist affected data subjects.

For instance, consider the record British Airways fine of $230 million. In 2019, British Airways was fined by the UK's data protection authority, the Information Commissioner's Office (ICO), for a breach that harvested personal and payment data. Circling back to Equifax, the organisation was fined only £500,000 ($625,000) in the UK for its 2017 breach, which was the maximum fine allowed under the pre-GDPR Data Protection Act. This figure, however, now stands at over $700 million, if you add the settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), and all 50 US states that claimed damages against Equifax.

Hardus Dippenaar, Senior Network Architect within Datacentrix Cisco business unit

> **"Businesses of all sizes must take a holistic approach to cybersecurity, looking not only at securing the environment, but also securing context, person, content and access."**

It's safe to say that the cost of a breach is increasing as you read this, and the likelihood of compromise is following suit. As the world takes data privacy more seriously, we see escalating fines by data privacy regulators globally. The rhetorical question then is, does this cost risk warrant a spend of between four and nine percent of IT budget only?

"Clearly, South Africa's financial industry has not escaped unscathed, with SABRIC announcing at the end of October that local banks are under sustained distributed denial-of-service (DDoS) attacks," adds Hardus Dippenaar, senior network architect within Datacentrix' Cisco business unit.

"And with our SMEs also being increasingly targeted by cybercriminals, businesses of all sizes must take a holistic approach to cyber security, looking not only at securing the environment, but also securing context, person, content and access."

For more information please contact Hardus Dippenaar, senior network architect within Datacentrix' Cisco business unit on 087 471 5000 or hdippenaar@datacentrix.co.za