Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Report Analysis

Databarracks: Data Health Check 2020

Databarracks has produced its ‘Data Health Check’ each year since 2008. It’s little surprise that this year’s report has a lot to say about the Covid-19 pandemic and organisations’ responses to it – predominantly the forced move to remote working. But it’s also a reminder that for the malicious actors operating in the cyber realm, it’s largely been a matter of business as usual.

Before getting into the pandemic issues, it’s worth looking at an issue that is barely touched on in the report, but which Peter Groucutt, managing director of Databarracks, was keen to highlight in an accompanying statement. According to the company’s data, ransomware attacks on UK businesses have increased 26% since 2018, and it’s an evolving problem.

“Cyber criminals are deploying more-sophisticated and innovative ways of extorting businesses and evidence shows this will escalate in 2021,” he said. “Outright prevention of ransomware is impossible, but it’s important that organisations learn from the new methods used by criminals in order to defend themselves.”

Among the new tactics commonly deployed is ‘double extortion’ in which, in addition to locking up data through encryption, attackers also extort it and threaten to make it publicly available, raising the possibility of even greater reputational damage and regulatory fines.

Many attackers are also biding their time, building in a delay between compromising and infecting a target’s systems and activating the malware. The idea is to ensure that the target’s back-ups are also infected, making it more difficult for them to restore systems and therefore more likely to pay up. And in some cases, attackers are targeting back-up systems directly.

“More companies will pay ransom demands, as the sophistication of attacks increases,” said Groucutt. “But paying a ransom does not guarantee you will get your data back. You must assume that you will suffer a successful attack. From that position, you have two objectives: to quickly detect and respond to limit its reach, and to bring systems back online and have the business operational as quickly as possible. It’s critical your incident response team or crisis management team has the authority to make large-scale, operational decisions to take systems offline to limit the spread of infection. The business must then find when the ransomware installation occurred in order to restore clean data from before the infection. Once the most recent clean data is identified you can begin a typical recovery, restoring data and testing before bringing systems back online again.”

Everything is dependent on having good back-ups, and this is where the report picks up.

Its sections on data protection and disaster recovery highlight that malicious actors are not your only problem. When it comes to data loss, hardware failure and human error still outweigh cyber attacks. And while it’s encouraging that 65% of the firms surveyed had actually tested their disaster recovery plans in the past year, that still leaves a third of firms that haven’t and which, therefore, have no idea how well – or if – they could survive a major disruption.

Interestingly, of the organisations that had tested their disaster recovery plans, more than three-quarters (77%) had specifically done so in the context of cyber threats. That’s up from 59% in 2017. It shows a shift in mindset, where hackers are increasingly seen as more of an existential threat to the business than, say, floods or earthquakes.

Arguably, the Covid-19 pandemic has been the biggest disaster, in terms of disruption, that most businesses have witnessed in a long while. From an IT perspective, the unavoidable shift to remote working for large numbers of employees hasn’t just created huge amounts of work provisioning and configuring the necessary infrastructure, it has also opened up the potential for significant security weaknesses. Some are obvious but difficult to address – such as the shear amount of corporate data that now has to move beyond the organisation’s perimeter. There’s also the issue of how that data is moving between the organisation and the employee, and which kinds of devices – locked-down and secured computers and smartphones issued by the company or the employee’s personal, and perhaps not so heavily protected personal devices. Many of the vulnerabilities that all of this confusion introduces will become apparent over time, as either security staff or hackers find them.

A little under two-thirds (61%) of companies had a tested business continuity plan in place. However, of those, a slightly higher percentage (66%) did not have any plans to deal with a pandemic. (The fact that some did is actually quite impressive.)

According to the report, the pandemic has hit companies in a number of ways. Half have lost revenue. Nearly a quarter (24%) have made cuts to staff pay. Just under half (43%) have reduced staff hours and 13% have made redundancies. In addition, a third of companies had suppliers who have gone out of business as a result of the pandemic. Most people’s definitions of ‘disaster’ would include a situation like that.

What does all this mean? If nothing else, Covid-19 will have broadened most IT practitioners’ understanding of the word ‘threat’. And the past year has underlined that organisations need to protect themselves from threats coming from many directions. Some of the traditional means of strengthening your organisation against these attacks – back-ups, disaster recovery planning and business continuity – continue to offer some of the best value for your security budget.

The report is available here: https://datahealthcheck.databarracks.com/2020/.