CYBER RISK GROWS AS CRIMINALS EXPLOIT CORONAVIRUS CRISIS

The coronavirus crisis is shuttering schools, businesses, and entire communities in an effort to slow the spread of the pandemic

Paul Mee and Rico Brandenburg

Cybercriminals have begun to actively exploit this crisis, with millions of employees now working remotely, security and IT teams subject to new and heightened demands, supply-to-demand volatility, and escalating psychological stress.

In recent days and weeks, we have witnessed a significant uptick in email scams and malicious website domains using the pandemic as a lure, as well as attacks with targets as high profile as the computer system at the US Health and Human Services Department.

Fortunately, there are strategies and practical steps businesses, management, and workers can take to help reduce the impact of heightened cyber risk to their organization.

THE MOST VALUABLE TARGETS

Several factors are contributing to the current crisis. Businesses and employees are stressed by the human and financial implications of the pandemic. Entire companies, school districts, and government agencies have shifted in just days to remote working, often overwhelming existing infrastructure and associated support systems. Even the most prepared companies that have advanced security, communications, and control capabilities will never have encountered this array of crisis-level challenges before. Cybercriminals are exploiting companies that are already under tremendous stress, proliferating malware inside of coronavirus news and desperately needed information packs, and extorting organizations to pay ransomware to ensure business continuity through the pandemic crisis.

Some of the most vulnerable targets include critical infrastructure providers, such as those in healthcare, energy, and financial services. Businesses that provide critical, highly sought-after services, such as utility companies, government agencies, and online streaming platforms, are experiencing far greater demand than normal and are feeling significant strain.

And, given the interconnected nature of supply chains and increasingly seamless digital commercial ecosystems, organizations need to consider where weak links may be in their supply chains, regardless of size or type of business. Those smaller and medium-size enterprises, which often lack sophisticated capabilities, are particularly vulnerable as they pause business-as-usual activities due to government dictate or quickly find means to migrate employees to remote working.

CHALLENGING TIMES

While business continuity, and even survival, has become the key priority, companies and employees are now exposing themselves to significantly increased cyber risk. Under high-stress scenarios, we are more likely to observe exceptions to security standards, such as the use of personal devices and public Wi-Fi networks, each with a significantly lower level of security protection relative to typical corporate infrastructure.

Even conscientious workers may unintentionally add risk by moving data, for pragmatic purposes, onto unsecured computers and personal devices. Potential exposure of sensitive information heightens legal and reputational risks with the exploitation of certain information going undetected where computers are not appropriately secured and monitored.

Where cyber incidents do occur, companies face difficulties communicating and executing quick and coordinated responses. Remote working will potentially challenge security teams in their ability to comprehensively identify threats and to isolate, protect, and, where needed, restore services and good data following an attack. Additionally, with an expectation that up to 60 percent of the adult population could become infected with the coronavirus, the health and well-being of the security workforce must be considered and backup plans established and tested. Even redundancies may be challenged, especially if there is limited geographic diversification of facilities or if multiple locations are simultaneously impacted.

As the crisis lingers — and based on our own analysis, scenarios of more than six months of major disruption are plausible — many corporations will look to reduce their workforce and, with that, the likelihood of disgruntled employees increases. Combine this with challenged security controls when working remotely, and insider risk will increase. The time for heightened diligence in this regard is now.

An organization is only as strong as its weakest link, and third parties have typically been a key area of vulnerability. Third-party suppliers and vendors will face the same challenges raised above. In some instances, they will be amplified by disrupted cash flows, lower level of preparedness to address the heightened risks, and/or high pressure in meeting evolving customer needs amid supply-chain challenges. It will be important for an organization to communicate and have visibility into its third-party vendors' security status to understand their increased security risk.

TAKING ACTION

There are a number of things an organization should and must do. We consider that there are at least five areas that should take priority.

Review business continuity plans and develop playbooks to account for the new challenges. These efforts should include, but not be limited to, preparing for the temporary or permanent loss of key staff and leadership, the evacuation of a security operations center, or a serious attack where only a portion of staff are able to work.

Increase awareness among the workforce regarding the risks of handling confidential or sensitive information when working remotely by being proactive in communicating and coaching teams on organizational policies and the best "dos and don'ts."

No organization or business is an island. Engage with peers and relevant industry groups to ensure insight on threat intelligence and best practices.

React quickly to this "new normal" by reassessing risks and ensuring that detection, response, and mitigation efforts are aligned accordingly. Review the security status of the most critical third-party suppliers and vendors, and be prepared to strengthen oversight. Tighten security controls across the highest risk areas, and apply tactical controls to mitigate increased insider threats by rogue or naïve employees.

Rapidly test the readiness of management, security, and the organization more broadly for this new way of operating. Examine preparedness levels by running drills for the main cyber risks that recognize new constraints, practices, and procedures (such as working remotely) and with potentially fewer resources and less expertise available.

The weight given to these actions will vary depending on the criticality of the organization to the citizens and security of a nation, as well as the operating model, distribution, technology, and culture of the organization — plus several other idiosyncratic factors, weaknesses, and exposures.

Overall, a stark reality remains: Organizations must combat the present coronavirus crisis on multiple fronts. And, in doing so, management needs to take all necessary steps to ensure business continuity through the pandemic, with the organization being fully prepared to deal with the heightened cyber risk associated with this unprecedented global event.

Paul Mee leads the Oliver Wyman Forum's Cybersecurity initiative and is the head of the Cybersecurity practice.

Rico Brandeburg, leads the Oliver Wyman Forum's Cybersecurity initiative and is a partner in the Cybersecurity practice.

This article first appeared on BRINK.