With the increase in remote work, businesses need to protect themselves against cyberattacks

The COVID-19 pandemic and subsequent lockdown have forever changed how we socialize and conduct business. More and more, our personal and professional lives will be online.

Paradoxically, our office towers sit empty. However, the amount of traffic in the virtual world continues to increase exponentially. Our physical borders are closed, but the virtual ones remain wide open, and relatively undefended. Cybercriminals — callous opportunists of the worst kind — take advantage of crises to engage in even more attempts to penetrate computer networks and extract data.

Phishing, smishing (SMS phishing) and vishing (voice phishing) attacks are all on the rise. Our tendency to click on infected emails has increased with the correspondent increase in email traffic — a two-fold impact on the severity of the threat environment.

New work spaces

In the past, knowledge workers might have been centralized into one, or a few locations, with controlled access to information. Now they are are dispersed across thousands of sites that the enterprise has no control over. Face-to-face communications are taking place on open, web-based platforms like Zoom, bbCollaborate, BlueJeans, GoToMeeting, Google Meet and many others, all vying for market share in an attempt to become the industry standard.

Concurrently, managers in organizations are dealing with unseen reductions in business volumes and making the difficult decisions of laying-off employees, shutting down plants and stores, and yet somehow still maintaining some kind of presence and level of customer service in the hope of recovering losses once the pandemic response restrictions are eased.

The challenges for enterprises of all kinds, then, are many: How can they maintain service levels while managing cuts and workarounds?

How do they provide employees with the equipment, tools, resources and information to work from home?

How do they balance restrictions from the lockdown against recovery when it lifts?

How do they support employees and protect them from burnout, exhaustion and other mental health issues? This is especially true for administrative front-line workers like those in information technology (IT) who are now responsible for maintaining secure, fully operational and accessible virtual work environments.

Staff who work in information technology for businesses are dealing with extra demands on their time and expertise. (Shutterstock)

Adapting for cyber-resiliency

The “start, stop, continue” approach offers a powerful structure to frame possible answers to the questions and dilemmas surrounding cybersecurity. Here, I offer three things to start, two to stop, and three to continue to ensure strong cyber-resilience is retained.

START: The most important thing to start is to monitor internal and external security threats and incidents. A few months ago, most of us had not even heard of Zoom, much less used it on a daily basis for both work and social gatherings. Most of us were not used to working from home, accessing work files remotely, uploading and downloading gigabytes of data. Most of us did not have more than rudimentary security on our home routers and networks. Most of us only had a passing knowledge of the IT support staff at work (usually called in a panic).

For managers and executives, this means daily reports on security incidents, their sources (internal or external), their nature and whether new types of attacks and attackers have been observed.

Enterprises also need to start asking themselves about the impact this new work environment has had on customers, employees, suppliers and other stakeholders. Executives should monitor what is being adjusted, and how. For example, to what extent are access permissions (to databases, files, systems and information) being increased? Concurrently, to what extent are insider monitoring programs being deployed to ensure employees do not inadvertently, or deliberately leak confidential or proprietary information?

Finally, the time has come to start enhanced online security protocols and tools, like multi-factor authentication, which only 57 per cent of enterprises are using.

STOP: In dealing with the new, distributed and virtual operating environment, organizations should first immediately stop or suspend any non-critical IT projects: this is not the time to continue with replacement of administrative systems, access systems, enterprise networking enhancements, application development or any other project aimed at changing or enhancing business processes.

There are two reasons for this. First, IT staff burnout increases exponentially in the current situation. They are dealing with a deluge of requests to configure home systems, manage access, provide ad hoc and formal training and deal with emergency shutdowns, not to mention an increased risk of breaches. They are not only at risk of burning out, but of making critical errors if they are also asked to continue non-essential development work.

The second reason is that hackers and other criminals will deliberately target organizations that are attempting to juggle remote staff support and IT development, perceiving these organizations to be weak, unfocused and inattentive.

Shadow IT are information systems or applications that individuals or departments use without the knowledge or support of IT staff in the organization. For example, a marketing manager may prefer to use privately sourced customer relationship management software that they find more accessible and modifiable, without the need to submit change requests to an IT department. The problem with shadow IT is that it has not been vetted for any potential security vulnerabilities. In the event of a breach, system administrators may not be notified or able to contain the breach if it emerges from a shadow system.

CONTINUE: Most organizations have well-developed crisis response plans as part of their enterprise risk frameworks. These documents need to be updated to reflect the new circumstances. Organizations

need to contact their insurance providers — including for cyber-insurance — and third-party support providers to alert them to their new operating environment. Like the enterprises they serve, these insurers and providers are also trying to cope and may be temporarily overburdened. Finally, organizations must continue to rehearse and update these plans.

Executives need to continue monitoring resources in their organizations, and where necessary, rapidly adjust budgets, staffing levels and other resources, allocating them to those areas that most need them. This might mean re-allocating IT development budgets and staff to cybersecurity or plant and office maintenance to supporting remote work environments.

Finally, executives need to ensure that succession plans for key staff are current. This is especially true for IT and cybersecurity personnel.

Preparing for the unknown

COVID-19 will prove to be a generational event with long-lasting and as yet unknown effects on society. By critically considering and discussing what to Start, Stop, or Continue with regards to cyber-resilience, businesses and their employees will be in a better position to anticipate, mitigate and flourish in current conditions and beyond.