Author: Jeff Clemons
Director of Risk and Cyber Advisory Services
March 26, 2020

Cybersecurity in Times of Uncertainty

The current pandemic has created an uncertain business environment. Companies are engaging with complex problems to balance employee safety with ongoing business goals and priorities. Meanwhile, there are individuals and groups prepared to take advantage of the situation by attacking what can be perceived as a weakened and distracted workforce.

We at Frost want to provide our clients and contacts insights into the risks associated with the current situation and the likely new world which we will all subsequently occupy. Specifically, understanding your attack surface, how fear can be exploited by outside forces, the strain of outdated technology on operations and the dangers of inadequate business continuity planning.

CURRENT RISKS

Expansion of the Attack Surface

With limitations of social gatherings and the closing of schools and businesses, companies are forced to accelerate their reliance on remote operations. As a result, businesses attack surfaces – any point of entry vulnerable to a hacker - are expanding quickly and in ways which IT functions may not anticipate. From additional reliance on mobile devices (laptops, tablets, phones, etc.) to the increased utilization of remote work applications, each additional login and system presents a different attack vector to your systems and data. Primarily, attackers are focused on exploiting weakened surfaces such as:

- Overloaded virtual private networks (VPNs) not being used by frustrated employees
- Sensitive files and data saved or accessed on un-hardened/un-sanctioned mobile devices
- Public and/or unsecured wireless networks being used to send and receive business communications and data
- Personal devices being used in lieu of provisioned devices for company communications
- Utilization of personal email accounts, file sharing services and communication platforms (WhatsApp, iMessage, Dropbox, Skype, Facebook Messenger) to transmit and receive data

For each of these risk areas, the expansion of the attack surface is often a result of your employees striving to find the most efficient way to work. These risk areas will become more common and apparent over time. Just as it takes time for individuals to be diagnosed, it will take time for businesses to realize and report the scale of any attacks on their systems and data.

Technology Obsolescence

As with the expansion of the attack surface, existing remote technologies will be pushed to meet increased employee needs not normally experienced or planned for. At offices around the world, desktop computers, antiquated phone systems, peer-to-peer local area networks and paper media are still relied upon by employees to conduct work on a daily basis.

Author: Jeff Clemons
Director of Risk and Cyber Advisory Services
March 26, 2020

Cybersecurity in Times of Uncertainty

While some industries (finance, telecom, hosting providers) require the security and other industries (manufacturing, distribution) demand the convenience associated with a non-remote workforce and technology, most businesses have been required to maintain the status quo by adapting a reactive technology strategy to meet the needs of office-bound employees and businesses. Long-term, a reactive – rather than proactive - position sacrifices growth and efficiency, while focusing costly and limited resources on technology, policies and procedures that hinder productivity and frustrate end-users (employees).

Fear Exploitation

Phishing campaigns focusing on the COVID-19 virus are cleverly designed to take advantage of the fears of employees. In recent weeks, the number of emails, text messages and phone calls that exploit these fears and the desire for information have increased exponentially, focused on vulnerabilities in the expanded attack surface. Specifically, these campaigns take the form of official company announcements, emergency service communications and links to viral media messages and videos. These methods aim to obtain access to devices (malware/viruses) and/or networks (stolen credentials) or business data not normally accessed or processed outside of the confines of a traditional office. Training employees to recognize social engineering attempts is necessary in day-to-day operations and is even more important during times of increased public and company uncertainty.

Inadequate Planning and Response

In the past, businesses have focused their continuity planning on responding to disasters and the associated timely resumption of interrupted IT operations through the restoration of systems and data. With the uncertainty related to the current pandemic, these traditional strategies and timelines for resuming normal operations are both insufficient and unclear; traditional business continuity strategies must now be pivoted to address long-term reliance on remote operations. As part of this shift, business continuity plans and responses must embrace a commonly neglected aspect of any plan: how non-technical employees can be continuously supported over a continued change in operations. Effective communication between executive management, the IT operations team and application users is more important than ever.

ADDRESSING RISKS

We appreciate that our firm and our clients are having to adapt to a situation that is uniquely uncertain and requires a timely and decisive response. This response to crisis provides an opportunity for businesses to learn lessons under pressure which can improve existing capabilities and lead to an embrace of new ways of doing business. These risks can be addressed in the following ways:

- **Acknowledging that traditional IT planning and strategy must be adapted to focus on business operations rather than just IT infrastructure and data.** Continuity must utilize a holistic approach that is formed and managed by company leadership to address the execution, monitoring and communication required by employees and customers to meet business needs.

Author: Jeff Clemons
Director of Risk and Cyber Advisory Services
March 26, 2020

Cybersecurity in Times of Uncertainty

- **Adoption of an IT culture that enables the utilization of applications and environments that can be continuously used by both remote and in-office personnel seamlessly.** Employees are already the weakest link in a business' cybersecurity methodology; remote employees will only exacerbate the need for an adaptive deployment of secure tools for a business to resume normal operations. Businesses should rethink how end-users interact, perform their jobs, and access current systems and data. Barriers seen as overly restrictive and outdated are typically the ones exploited and circumvented by employees (and thus, attackers) first.

- **Implementation of enhanced cybersecurity training which clearly communicates risks to remote employees.** Training should focus on employees' ability to respond and exercise their judgement while proactively identifying the risks they face. While any cybersecurity training reduces risks, training that includes both IT and the impact of cybersecurity on a company's operational and financial policies and procedures will exponentially reduce overall risk to a business operating in a remote environment.

- **Engaging a proactive - rather than reactive – strategy for addressing end user IT needs.** Traditional strategy typically requires IT personnel to maintain existing environments that were usually developed to meet past needs and requirements. Maintaining current operations should be a key responsibility of any IT department; however, maintenance should only support improvement and adaptation of the environment to meet end-user needs. Company leaders should re-evaluate current IT operations to determine if their IT personnel and strategy can meet these needs, acknowledging the possibility that external parties can be utilized to shift the strategy of IT departments to a proactive, end-user focused function.

About Frost's Risk and Cyber Advisory Services

Frost Risk and Cyber Advisory professionals provide you with in-depth cybersecurity knowledge and experience facing your business in today's challenging environment. For more information on how Frost can help you, please contact Jeff Clemons, Director of Risk and Cyber Advisory Services, at jclemons@frostpllc.com.

FROST, PLLC
Certified Public Accountants