MARSH

INSIGHTS | AUGUST 2020

Adapting Cyber Incident Breach Response Plans for the Remote Workforce

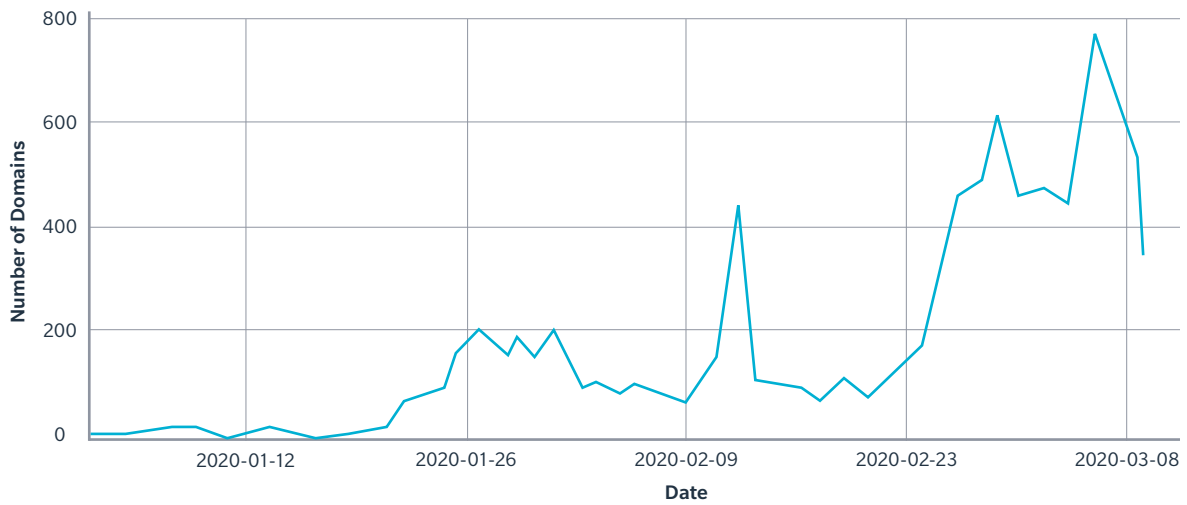
The COVID-19 pandemic prompted many organizations to rapidly move to a remote workforce, which often required IT teams to quickly expand the available network bandwidth and to modify the "normal" operating model to keep the business running. In supporting significantly more remote workers, IT teams may have bypassed their normal processes and procedures, thereby likely violating, weakening, or eliminating their IT and security policies.

In implementing their remote working solutions, organizations have inadvertently increased operational risk, especially in cybersecurity. Bad actors have been quick to capitalize on these risks, exploiting common VPN vulnerabilities, directing phishing campaigns toward users of popular communication and collaboration platforms, targeting Microsoft's Remote Desktop Protocol (RDP), and standing up infrastructure to support malicious campaigns (see Figure 1 below).

FIGURE 1

COVID-19-related Domains Created per Day

SOURCE: *RECORDED FUTURE*.



MARSH & McLENNAN COMPANIES

Due to the larger remote workforce environment, should your organization reconsider how to respond to a cyber-incident? Yes, and here's why.

Pre-pandemic, cyber incident breach response (CIBR) plans assumed the majority of employees would be working on-site in corporate-controlled environments. Now, many — if not most — employees are working remotely in a wide variety of settings. These non-corporate environments can introduce a host of new threats that IT and cybersecurity teams must prepare for.

As IT and cybersecurity teams tighten up their organizations' cybersecurity, they may not have considered their CIBR plans and how to adapt them to the "new normal" and the cyber incidents that may yet occur.

Security weaknesses are inherent in many home networks, which are typically "plug-and-play" and designed to operate with few configuration options when users deploy them. Physical security cameras, appliances, light switches, light bulbs, stereo components, baby monitors, and other common devices are generally set up to automatically connect to any available home network; these devices use a wide array of protocols and ports to communicate with manufacturers and users to provide convenient — yet insecure — services. And these same networks that are burdened with peripherally connected applications are the very same ones that remote workers are using to connect to corporate IT networks, which may or may not be connected to VPNs.

How can you better prepare for cyber incident response in remote environments?

As large-scale remote work becomes part of the new normal, it's important that IT and cybersecurity teams prepare for the potential exploitation of new remote infrastructures. Specifically, you should consider:

- **Identifying your weaknesses:** Develop a worst-case cyber scenario that involves a remote worker IT system malware event, and then conduct a tabletop exercise using this scenario. At the end of the exercise, identify what went well and what didn't, and assign staff to address any gaps and weaknesses in your CIBR plan within an agreed upon timeline. Your CIBR plan should then be updated accordingly.

- **Reviewing your baseline configurations:** Revisit the implementation of a minimum acceptable remote workforce IT system baseline configuration that limits the acceptable activities of the IT system. For example, consider eliminating the use of USB ports or restricting them to specific users who may need access as a part of their roles and responsibilities. Once the baseline is established and tested, roll this out to your remote workforce.
- **Implementing reviews of remote IT systems and other logs more frequently:** Consider the implementation of additional remote worker IT system logs that collect and analyze data to identify unauthorized or questionable activity that may require further investigation. Automate this audit log collection and analysis where possible.

When planning your response to a potential CIBR incident while your workforce is largely remote, it's important that you:

- Develop processes and procedures needed to isolate individual remote IT systems — or a group of IT systems that may work together — to support requisite cyber analysis and investigation.
- Determine how remote IT system cyber forensics would be conducted, including chain-of-custody procedures.
- Be prepared to quickly collect remote IT systems logs and imaging of remote workers' hard drives.
- Consider how to get selected remote workers back online as quickly as possible (if required).

Preparation, planning, and conducting cybersecurity tabletop exercises — both technical exercises and those involving senior management — will go a long way in helping your organization tap into the benefits of your remote workforce while being prepared to efficiently and effectively deal with cyber incidents.

For more information, contact your Marsh representative or:

RUBY RAI, CIPP/C, CRM
Cyber Practice Leader
+1 647 220 2871
ruby.rai@marsh.com

GREG ESKINS
Canada FINPRO Leader
+1 416 868 2768
gregory.eskins@marsh.com