THE BIG SECURITY DECISIONS FACING CIOS IN 2021

January 20, 2021 • Forbes • Kevin Beasley

CIOs and their teams are overwhelmed from managing the massive effort it took to make their operations remote, but now is not the time to pause.

A spike in ransomware and phishing attacks has hit organizations from hospitals to payment processors and has left many IT operations reeling. A recent analysis revealed that more than half of major cyberattacks involved ransomware — leading to a C-suite nightmare of technical untangling and scrambling to save face with clients and employees. Making matters even more urgent, attacks are thriving in the wake of a mass migration to remote work and sometimes because of the patchwork system architecture put in place quickly to keep businesses running.

Over the next year, CIOs will have several more critical decisions to make to secure this new remote environment. The hard work is not over yet, but these decisions will be much easier if you know what to expect.

It's a good bet that many CIO's did not have "global pandemic" in their cybersecurity playbook for 2020. But if the pandemic taught us anything, it is to prepare for everything when it comes to threats. Over the next year, CIOs will be a critical part of updating business continuity planning (BCP) and conversations and will also be expected to answer for any potential breaches or threats that emerge. During this time, CIOs will need to make several key decisions. Consider the following while weighing your options:

Unchecked remote access and dated protocols are risky. The more disparate networks your architecture connects, the more ways you are at risk. A surge of ransomware attacks during the pandemic have exploited mapped and unmapped network shared drives, holding the data of many small- and medium-sized businesses hostage. Additionally, phishing attacks are increasingly tricking users into revealing their password hints — mother's maiden name, city of birth, etc. — as bad actors attempt to compile enough information to breach systems. This kind of social engineering takes many forms but has a common solution: education.

You should ensure employees continue to get the IT support and information they need to operate safely in a remote environment and reduce risk to the larger organization. Further, you will need ongoing education for yourself and senior leadership about the latest threats. One solution would be to discontinue the use of protocols such as SMB and FTP and instead use protocols such as WebDav, HTTPS and FTPS/SSTP. If mapped drives or any other vulnerabilities exist within your tech ecosystem — even with the best security products in place — you must move swiftly to shore them up or remove them. Ultimately, you

will also need to secure buy-in for investment in new tools or services that can mitigate these threats.

Put plans and procedures on paper.
If a breach occurs, how is it communicated to you? Do you have a minute-by-minute breakdown in your disaster recovery plan of your response to a ransomware attack documented? Are you confident you are up to date with all the jurisdictions and regulatory bodies that you must report a cyberattack to and what kind of process that requires?

Critical decisions with steep consequences occur at a breakneck pace during an attack. While the dwell time of malicious code has dropped as organizations spot attacks faster, bad code still does significant damage in the 79 days it lurks in systems on average. Commit to formal, documented policies and processes regarding incident response and BCPs in 2021 and account for as many scenarios as possible. CIOs would not want to go through the scramble of ramping up their organizations for remote work again. With a dedicated plan for business disruption, the response to the next crisis won't be a fire drill.

Be equipped for transparency.
If an attack occurs, a quick and strategic response is imperative. Aside from making technical decisions in real-time as CIO, you will also be responsible for informing the messaging intended for clients, internal teams and the public. This cannot be done without a holistic view of your organization's systems. If you find yourself in the unfortunate situation of being technically outmatched by a breach or ransomware attack, enlist the help of a respected third party to thoroughly investigate and help reassure clients you are taking the situation seriously.

Remember insurance only goes so far.
Most CIOs have heard a pitch or seen a targeted LinkedIn ad for some form of cybersecurity insurance. The investment is tempting. For organizations with an already strong security program of their own, it can be a "peace of mind" investment or yet another fail-safe against something unexpected. But it cannot be your entire security strategy. Many of these policies have fine print and stipulations that require significant IT due diligence on your end to pay out — so there is no guarantee you'll be protected. Instead, if you are required or prefer to have insurance, you should protect your investment on premiums by reinforcing internal practices.

CIOs are still in the thick of a critical decision-making period as we enter 2021. The more informed you stay about what is ahead, the less likely you will get caught off guard. A global pandemic may have been low on everyone's cybersecurity threat list, but we have now learned the lesson that no proactive security plan is a wasted investment.