FPLG
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

Quarantined Nonprofits: Cyber Security Worries

10.21.20 | Linda J. Rosenthal, JD

As COVID-19 quickly engulfed the United States in mid-March, the normal world of work as we knew it evaporated.

Faced with lock downs and quarantines, much of the activity in the for-profit, nonprofit, and government sectors stopped entirely or abruptly switched off-site.

The sudden move to remote operations was just one aspect of this enormous pandemic calamity. Initially, the focus was on the daunting details of hooking up and configuring electronic and communications hardware and software in millions of private homes. And, for the many workers who lacked adequate technology or broadband, their employers had to scramble to fix that obstacle. Along with these changes, came new and different security concerns.

But, all too often, the matter of security was forgotten entirely, misunderstood, underestimated or brushed aside until later.

And that's a big problem.

Cyber Dangers

Not surprisingly, this dramatic change also took the cyber criminals by surprise. Initially, they had to scramble and adapt; it appears, though, they have managed all too well.

"While the COVID-19 pandemic has radically changed the landscape of how we live and work, one constant has remained: Cybercriminals are taking advantage of chaotic situations for their benefit." That's the warning from Roger Rustad of TechSoup in *Nonprofit Remote Security During COVID-19* (July 9, 2020).

Before the pandemic, it was clear that threat actors attacked a variety of targets, large and small. Now, hackers are apparently capitalizing "on the current situation [by] attacking a wide range of targets indiscriminately. So, just as before, it's critical for nonprofits of all sizes to take reasonable security precautions. See *Keeping Your Nonprofit's Systems Secure During the COVID-19 Pandemic* (April 3, 2020) Linda Widdop & Michael Enos, *TechSoup Blog* [includes important tips especially for small nonprofits]

Of course, the danger comes not *only* from malevolent outside hackers but from unscrupulous insiders as well. It comes as a surprise to most people that embezzlement and fraud by people associated with nonprofits has always been a problem. See *Charity Embezzlement: Thwart It With Good Controls* (November 17, 2016). The difference now is that the manner of embezzling is changing; indeed, our reliance on technology presents easier access for insiders with computer skills to commit these crimes.

Cyber Security Challenges

By mid-summer, there were both anecdotal and formal reports of how well most entities that moved to remote operations were faring. A study of a wide variety of businesses by technology firm Malwarebytes gives insight into successes and areas to make improvements. (The findings transfer generally to the nonprofit sector.) See *Enduring from home: COVID-19's impact on business security* (August 2020) Malwarebytes [Report]; *How the shift to remote working has impacted cybersecurity* (August 20, 2020) Lance Whitney, techrepublic.com [article discussing the study findings].

Among the areas shown to have been inadequately addressed are: cyber security training focused on the particular threats of remote operations; analyzing "the security or privacy features in the software tools considered necessary for remote working"; and failing to "deploy a new antivirus solution for work-issued devices."

Almost half of the respondents said their "biggest concern was that devices may be more exposed at home where employees feel safe, but those devices could be accessed by other people who could accidentally compromise them." Complicating the security issue further, it's now clear that many workers use a *combination* of the work-issued and personal devices – no matter what their employers set as policy. "Employees may not have adequate cybersecurity protections for their personal networks and devices."

Other problems include:

- Workers "may be using unauthorized and unmanaged 'shadow IT' tools to share employer and customer data
- Remote work appears to increase the risk of malware, phishing, and ransomware attacks
- Tools now frequently used that involve cloud collaboration (like Zoom and Slack) "may not provide adequate cybersecurity"

Reassess Cyber Controls

In *Strengthening Internal Control in the COVID-19 Environment* (October 19, 2020), Cara DeMartini, CPA, of BDO USA emphasizes that even if a nonprofit organization had implemented early and

apparently adequate new practices and policies, it should reevaluate whether changes or improvements are needed.

"[A] strong internal control system," she writes, "has always been a priority for audit committees and management of nonprofit organizations. They've established policies to address the primary question — 'what could go wrong?'" Now we know: the many COVID-19 challenges include "a scattered and remote workforce."

So "management of nonprofit organizations are asking themselves — are the internal controls that were once effective still operating in a manner to achieve our objectives in this unprecedented time? What can nonprofit organizations implement in order to adapt to this remote environment, when their employees, resources, technology and documentation may only be accessible through virtual means?"

Ms. DeMartini offers several tips for nonprofit management to consider to strengthen their "internal control environment in response to a remote environment." In particular, regarding "new cybersecurity and data integrity risks" arising from off-site operations, she advises nonprofits to reevaluate their risks and then *reassess* any existing security controls based on the new analysis.

She also strongly recommends seeking advice and help from outside experts; they will be more up-to-date in current "best practices" for the COVID-19 remote-operations issues.

Conclusion

See our last month's post: *Blackbaud Data Breach: Fallout for Nonprofits* (September 29, 2020) as well as an upcoming one on steps to take in light of the massive Blackbaud breach.

— Linda J. Rosenthal, J.D., FPLG Information & Research Director