Business Email Compromise Commonly Asked Questions

1. Should we all be switching away from email, at least for internal communications, to more secure tools like Microsoft Teams?
   Tools like Microsoft Teams, Slack, and others provide a medium through which employees can quickly and easily collaborate and communicate with each other. In many cases, using these tools for instant messaging makes more sense for quick and casual communication. Adding these tools to your mix of technologies can add some real benefits. However, these tools work best for one-on-one communication or communication amongst small teams and can be chaotic for bigger organizations. But from a security perspective, you will never be able to replace email. You may be able to influence internal behavior to move away from sending emails, but you will need to be able to receive emails from external parties and therein lies the risk. The best solution is to try to secure email as best as possible and train your employees on cyber risks. - ND
2. What's a good first step to protect a company with limited time/resources?
   Develop a written information security plan (WISP) as required by law for all Massachusetts businesses. The WISP should include a set of technical and operational requirements that embody useful data protections. The company then can continue to improve it during required annual reviews or following a breach and can also test the protections by retaining third-party security audit firms. - RM
3. How can a company evaluate its current exposure and plans against attackers who have state-of-the-art technology?
   Some hackers have state-of-the-art technology, but most of them are lazy, relatively low-skilled and are looking to make a quick buck with relatively basic tools. An analogy that fits here would be a thief walking down a street late at night looking to steal from unlocked cars. They are not targeting your car specifically, but if you didn't lock your door, you become their victim. For most companies, simply locking the door (for our analogy this means employing basic cyber hygiene) is enough to deter most hackers. We recommend bringing in an independent third-party to perform a baseline cybersecurity assessment. This would provide you with an initial measurement of your current security posture and give you a prioritized risk-rated direction to improve your organization. - ND
4. For regular, non-financial businesses, what are best practices to avoid wire transfer or payment fraud?
   - Encrypt all outbound emails containing wiring or payment instructions, so they won't be accessed by bad actors;
   - Don't issue payments until the payor confirms internally through a secure non-email means that the payment to the payee is actually authorized; and
   - Don't issue payments until the payor confirms with the payee through a secure non-email means, typically a phone call, that wiring or payment instructions are accurate. - RM

(Continued)

5. What is the best way for a company to use its business partners in banking/law to address these issues?
   As your banking partner, we highly recommend periodic treasury management relationship meetings to review and confirm clients are aware of the latest cybersecurity threats, best practices to avoid business disruption, and actively using available fraud prevention tools to minimize exposure and potential financial loss. - MM

   With legal partners, involve a qualified data security attorney at the earliest practicable date. Legal counsel can help develop and/or improve required or recommended security policies and help manage response actions following potential breaches. - RM

6. What do you recommend for the best antivirus software?
   Antivirus and antimalware, generally part of what we call endpoint protection, are a crucial component of a defense-in-depth strategy. Some of the leading products out there for corporate environments are Microsoft's Defender ATP, Sophos, and ESET. However, keep in mind antivirus software is only one of many protection mechanisms your company should employ. - ND

7. What should we do if we don't have a cybersecurity person on staff?
   Small businesses often struggle with having the resources for a dedicated cybersecurity resource. Companies that don't have room on the payroll for a cybersecurity staff should consider an outsourced model. There are specific types of IT support companies known as MSSPs or Managed Security Services Providers. Many of them focus on helping small businesses and have flexible models of engagement so that the costs are reasonable. - ND

8. Where can I learn more about the Massachusetts laws on this topic?
   The key legal provision is 201 CMR 17, which requires all Massachusetts companies maintain a WISP with specific requirements that embody useful and important data protections. 201 CMR 17 has been in place since 2010, and commentary is widely available in an internet search. Additionally, security breaches are defined and addressed in Massachusetts General Laws, c. 93H, and the obligation to destroy personal information upon disposal is addressed in Massachusetts General Laws, c. 93I. As always, your attorney can be a great source of information and provide answers to any questions you have specific to your business. - RM

9. What resources can you recommend for staff training and mock phishing attacks?
   There are a wide variety of tools and resources that can help train staff and conduct mock attacks. Firms like DGC offer these services, as do many managed service providers. Some of the major simulated phishing attack and training platforms include Wombat and KnowBe4, which DGC resells and helps clients implement. Some other major platforms include Proofpoint, SANS, Cofense, Webroot, and Barracuda PhishLine. - ND

Contributors:
Nick DeLena, CISSP, CISA, CRISC, CDPSE, Principal, DGC - ndelena@dgccpa.com
Mike McMorrow, VP, CTP, Treasury Management Services, TD Bank - michael.mcmorrow@td.com
Rob Munnelly, Shareholder, Davis Malm - rmunnelly@davismalm.com

If you have questions about how to protect your organization from business email compromise, please contact Nick DeLena, CISSP, CISA, CRISC, CDPSE at 781-937-5191 / ndelena@dgccpa.com.