Banking perspective on fraud and cyber risk: ideas for protecting your business

Written exclusively for *Security Systems News* and first appeared [here](#).

By: Greg Buscone, executive vice president, senior commercial banking officer, Eastern Bank

As a career banker, protecting against fraud is top of mind regardless of whether we’re in a paper- or technology-driven world. Fraud prevention practices are at the forefront of considerations for customers given that they are entrusting us with their money. As their commercial banking partner, offering a lens to ensure they’re asking the right questions, taking the most prudent steps and applying a financially sound perspective to their fraud protection program is a unique value-add to their business.

The reality is that technology has made fraud more common, increasing the types and frequency of risks that are likely to impact your business. Creating and maintaining best practice security preventions for today’s ever-expanding range of threats help businesses minimize risk, ultimately benefitting the customers it serves.

When it comes to preventing fraud and cyber risk, I’ve seen many changes over the past 30+ years at the national, regional and community levels. What has remained constant — whether you’re a locally driven security alarms company or a multi-state operator — are businesses integrating a fraud protection program into their operations from a banking perspective.
What’s old is still new
Protecting your cash operations from check fraud is nothing new. With technology’s influence, one might think written check fraud would be declining but it is still common – precisely because of technology’s rising influence. In fact, 75 percent of organizations experienced check fraud in 2016, an increase from 71 percent in 2015 and a reversal of the declining trend in check fraud since 2010 (source: 2017 AFP Payments Fraud and Control Survey).

Business email compromise (BEC) scams are rising, targeting both wire and check payments. BEC scams are commonly spam emails that appear as a regular email from a CEO, CFO, vendor, business partner or close friend, for example, requesting a check transfer or other payment. They make it possible for email to get hacked. According to the FBI, BEC scams are “increasing, evolving and targeting businesses regardless of size or geographic location.” Reported losses associated with BEC scams have totaled over $12B since 2013.

The statistics are startling:

- Seventy-four percent of organizations reported they were exposed to BEC in 2017, a 10 percent increase from the prior year;
- BEC scams continue to grow at an alarming rate. As recently as 4.5 years ago, there was a 1,300% increase in actual and attempted losses;
- Sixty percent of companies that experienced payments fraud via BEC did so through wire transfers; and
- Ninety percent of all malware is still delivered by email.

So how can we move beyond the fear of an incident and focus on proactive security?

Positive pay is a tested, trusted and valued product for preventing check fraud and attempts. Used by businesses of all sizes and across industries, it notifies your bank daily of your checks issued for payment, processing only those listed. It’s an effective option for BEC protection, whether you are just starting to think about fraud prevention or are interested in enhancing your existing arsenal of tools with a product that can protect the basic cash management operations of your business.

To reduce wire transfer fraud, consider involving fewer parties as an underlying philosophy to your program. Have your bank set you up to conduct wire transfers on your own online system. This provides a safer method for managing communications with highly sensitive information, cutting down on the volume of email, which is always a good step to reducing the likelihood of a hack. Additionally, if you are feeling any form of doubt, call directly the parties involved to verify all communications and account information haven’t been tampered with and are correct.
What’s new is new
We are seeing more customers and prospective customers losing the ability to use their computers, access data and ultimately serve their customers due to the fallout from a ransomware attack. Ransomware is file-encrypting malware that typically infects a workstation through a phishing email, and can then quickly spread from the workstations to unpatched computers on the network. This can become very costly. When uninsured, businesses can pay upwards of hundreds of thousands of dollars to recover from a ransomware attack.

Preventing cyber risk is a shared organizational responsibility. Your technology department and technology service providers should have cyber risk products to protect and prevent attacks. Additionally, your banking partner can help you navigate fraud prevention with products and services to help minimize an incident. Your insurance partner can also offer cyber risk insurance to help mitigate the financial toll of an incident.

When speaking with our customers about fraud prevention, I guide our conversations around these core information security controls:

1. **How are you protecting your computers?**
   - A patched computer is only vulnerable to the most advanced of cyber attacks. What is your strategy for ensuring that both workstations and servers are patched at least monthly?
   - How do you ensure that every computer in your organization is running an anti-malware product, such as antivirus?
   - How often are you backing up your sensitive data and systems to assist recovery in the case of a ransomware attack?

2. **How are you protecting your email?**
   - What email spam or security filtering solution do you have in place?
   - What phishing training on BEC risks do you provide to employees who handle sensitive information or have access to send money?
   - Multi-factor access (MFA) can stop compromised credentials from being used. Do you require MFA when accessing email when not on company networks?

3. **When was the last time a third party tested your systems for security vulnerabilities?**
   - A third party may identify a security vulnerability before a malicious attacker. What is your cadence for regular testing?
   - Leveraging the same provider regularly will provide diminishing results and a lack of unique views. When did you last select a new partner for security?
The new frontier
Check and cyber fraud will only become more sophisticated and common in the future as our digital-focused world advances. How businesses assess, prepare and protect will make all the difference in minimizing their operational risk.

There are both simple and more extensive steps you can apply from a banking perspective to help prevent and protect against day-to-day issues. This includes layering in an evaluation of your internal information security practices with a banking lens. Demonstrating strong controls and practices for your banking operations is becoming increasingly impactful for securing business loans and growth capital for your company. Fraud and cyber security health are more important than ever for your overall organizational risk as well as financing and cash management options with your banking partner.

---

Greg Buscone is Executive Vice President, Senior Commercial Banking Officer at Eastern Bank, with responsibility for Eastern’s Commercial & Industrial lending portfolio which includes business customers focused on security systems and alarms. Founded in 1818, Boston-based Eastern Bank is America’s oldest and largest mutual bank with $11 billion in assets and over 115 locations serving communities in eastern Massachusetts, southern and coastal New Hampshire, and Rhode Island. For more information, contact Greg at g.buscone@easternbank.com.