Scotsman Guide
https://www.scotsmanguide.com/browse/content/practice-good-digital-hygiene

May 2020

# Practice Good Digital Hygiene

## Cybersecurity starts by implementing good habits within a company

By **Jeffrey Bernstein,**
Managing director, Marcum Technology LLC

Financial-services companies face an array of sophisticated external threats, including potential attacks from foreign hackers. The greatest cybersecurity threats, however, come from within the company itself.

Employees often make mistakes with data and devices, leading directly to a breach. In some cases, the consequences are not too severe, but the risk is always high. Easily preventable mistakes lead to catastrophic breaches every year. The problem is often due to corporate cultures that have missed an opportunity to educate staff on the importance of using good digital hygiene.

The term “digital hygiene” has been around for about 20 years and is especially fitting today, given the recent global coronavirus threat. Americans have been repeatedly warned to take a few simple, precautionary steps — washing hands, working from home, etc. — to protect themselves and prevent the

spread of the virus. We can think of cybersecurity in a similar way. A few steps can go a long way in guarding your data and preventing the wide-ranging, damaging effects of a major data breach.

**Understanding the risk**

It's not that mortgage companies aren't aware of cyber threats. Data protection is among the most dominant concerns for commercial mortgage lenders. Cyber incidents ranked first among the most feared global corporate perils as of fourth-quarter 2019, according to the Allianz Risk Barometer 2020 report.

This report was based on survey answers from 2,718 respondents from companies of all sizes in 102 countries. The noted risks included cybercrime, information-technology (IT) failures or outages, data breaches, ransomware, and penalties levied for noncompliance with legal and regulatory mandates.

Commercial and residential mortgage companies are making cyber protection a priority for various reasons. For one, there is increased pressure from regulators. Companies also have more at stake because they are doing more of their business online. The endless parade of publicly disclosed, high-profile cybersecurity breaches also has scared some companies into action.

Many commercial mortgage originators understand they are high-value targets. They know it is critical to properly secure their sensitive client data. They've already invested heavily in the latest security technologies to protect their computing networks. They've also adopted policies and procedures that help them operate efficiently while meeting legal and regulatory requirements.

Despite all these precautions, some of these same companies may suffer a major breach this year. The breach likely won't be caused by indifference to the threat or a flaw in the security technologies deployed to protect the data. It will most likely result from an employee mistake.

Security breaches are most often caused by employees who do something they shouldn't do, such as clicking a suspicious link in an e-mail, opening a malicious e-mail attachment, using weak passwords, losing portable devices with confidential data or being tricked into giving up their credentials through social-engineering attacks. The vast majority of successful data breaches begin with some type of human error, studies suggest. Because of this, educating staff on the importance of using good digital hygiene should be a key component of the security program for a commercial lending operation.

**Practicing digital hygiene**

But what is good digital hygiene anyway? Large financial companies typically spend a lot of money securing their data and systems. Small and midsize commercial mortgage originators won't have the same budget as large banks and nationwide companies. This makes them easier targets for cybercriminals. Fortunately, employees can be trained to practice good digital hygiene at little to no cost.

First, access to the data itself needs to be restricted in various ways. Sensitive information should be encrypted when it is collected, stored and transmitted. Data encryption means that the information is translated into a code that only those with a password can access and read.

Using multifactor authentication is another useful protective measure, whenever it is available. This essentially means that employees have to provide two or more levels of credentials when accessing an account, such as a password followed by a fingerprint or a pass card. A company also should require employees to use strong and unique passwords, as well as anti-virus software that updates automatically.

Employees need to be skeptical of all e-mails, text messages and attachments. Train your employees to verify the source prior to clicking on links and attachments. The company also should ensure that

computers and other devices automatically lock out users when left inactive for a certain period of time. Only authorized users should have access to a company's computers and network.

Companies should back up sensitive data and keep software updated, and avoid using unknown public Wi-Fi connections. Only use wireless networks protected by a service set identifier (SSID) and, preferably, a virtual private network (VPN) connection. Use only mobile apps from reputable sources, such as Apple, Amazon, etc.

If the user is unsure about the authenticity of an app, they should research it thoroughly prior to downloading it. Also, you should delete unused apps. Lastly, a company should configure devices to avoid shared connections from other users, and ensure that the various apps on mobile devices are locked down to prevent access to an employee's personal information.

Employees need to be told to speak up if they make a mistake. People should be told to seek immediate help from internal IT personnel when they've been compromised in some way. These simple and relatively inexpensive steps outlined above can go a long way in reducing the risk to your data.

• • •

Commercial and residential mortgage originators arguably represent the highest-value targets for cybercriminals. Mortgage companies collect a mountain of sensitive and valuable information in every transaction. Think about how much critical information is stored in a single loan file and then consider that several recent breaches have involved thousands of transactions. This is why a major data breach can be fairly likened to a pandemic.

Preventing a major breach is not unlike stopping the spread of a disease. Good digital hygiene is simply common sense and it can help lower the risk of some of the most common cyber-borne threats.