# Compliance is key if you file cyber-insurance claim

SCOTT TORNIO
GUEST COLUMNIST
TECHNOLOGY

Cyber Insurance has been a hot topic lately. Many companies started cyber policies in January and now are scrambling to fulfill their obligation by the end of Quarter 1. I can save you some trouble in telling you that they're not going to check for compliance unless you submit a claim. I can also tell you to read your policy as many of the things that were listed on your cyber insurance questionnaire are not actually in your policy.

The questionnaire probably asked you about the following:

**Multi-Factor Authentication (MFA) for email:** Multifactor Authentication or MFA (you may also see 2FA) is the process of using multiple means for logging into a system. Your password is one. Often a code received via text or from an app is another. Your phone uses your face as a secondary authentication method.

MFA for emails is almost certainly in your policy and if you experience an incident where your email is breeched, they will ask you to confirm that MFA was enforced at the time of the breech before paying out any claims. If you are using Microsoft 365 or any other cloud-based email system and you have some or all accounts without MFA do something about that now.

**Multifactor Authentication for VPN:** If you don't know what VPN is, then this probably doesn't apply to you. This one may be in your policy. It's been hit or miss on the policies I've read. MFA for VPN is most commonly provided through Microsoft Azure or through Cisco Duo. Some firewall manufacturers provide it directly (I believe SonicWall does), but most don't. Read your policy to see if this is a requirement. If you already use Microsoft 365, upgrading to Business Premium licensing will give you Azure controls, including MFA for VPN. Otherwise, look into Cisco Duo.

**Multifactor Authentication for privileged accounts:** This refers to IT administrator accounts. I have yet to see a policy that is actually enforcing this, but I am sure there are some out there. My understanding is that Microsoft Azure cannot do this one yet, which is weird because the administrator accounts are tied to Microsoft Servers. Cisco Duo, however, can do MFA for privileged accounts.

As a quick aside, I feel like Cisco Duo is a flash in the pan product. Time will tell and I could be wrong, but I feel like Cisco just bought a product to fill a void until everyone gets the technologies in place to provide MFA without it. Within a couple years, we shouldn't need Cisco Duo anymore. I only mention this because a lot of companies are investing in this solution now and we should all be prepared for the possible eventuality of having to do all of this MFA stuff over again when Duo becomes irrelevant.

**Employee phishing training:** This is a fun one. Phishing Training is a service wherein simulated phishing emails are sent to your employees in an effort to trick them. Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure such as ransomware .

Employees are enrolled in brief, web-based training sessions to better detect and avoid phishing emails. This one has also been hit or miss on policies but is becoming more hit than miss.

**Disaster recovery/Business continuity (DRBC):** Virtually all policies ask that the business have a DRBC plan. I and others have provided information on these plans so I'm not going to go into detail here. All I will say is that you need a plan. Your policy probably doesn't dictate how great of a plan it is or if the plan has been tested. To me, this is like returning your cart at the grocery story. A good, tested plan is the right thing to do and you should do the right thing even if no one is watching.

**Dark Web monitoring:** So, there is this thing, called the Dark Web. Long story short, it's a bunch of websites that aren't searchable by Google. It's mostly known as a place for criminals to exchange illegal stuff for cryptocurrency. There is more to it, but that's the gist.

The Dark Web monitoring service looks in the Dark Web for your accounts and passwords and lets you know if the bad guys compromised your account and are selling your credentials. Not a lot of insurance companies are requiring this, but it's still a good thing to have. Ideally, you are selecting good passwords and using multifactor authentication, so you aren't on one of these lists anyway.

There are other requirements possible depending on your business. The Health Insurance Portability and Accountability Act (HIPAA) and Personal Identifiable Information (PII) requirements could come into play if you are a medical business or business that keeps personal information on systems. I just listed the most common, that apply to virtually all businesses. Again, read your policy and work with someone that you trust to ensure that you are compliant.

Scott Tornio is president of HawkPoint Technologies.