SKYTOP STRATEGIES

CYBER RISK – NEXT STEPS FOR EVOLVING SECURITY?

*By **Christopher P. Skroupa** Posted February 26, 2018*

Originally published on Forbes.com

SKYTOP STRATEGIES

Christopher P. Skroupa: Are cyber security issues a C-Suite or I.T. problem, or do they expand beyond one focus?

Rich Frankel: Cyber security is an issue for everyone in all organizations, large or small. However, when you specifically talk about a CEO and the C-Suite, cyber security is – after some time – definitely an issue that they need to be fully aware of, and involved in when cyber security related decisions are being made.

Richard M. Frankel *served for more than 25 years in public service, and the majority of his career has been with the FBI. Serving as Of Counsel at Ruskin Moscou Faltischek P.C., Frankel's practice focuses on Cyber Security and White Collar Crime & Investigations. A recognized authority in complex investigations, asset recovery, cyber issues and crisis management, Frankel also provides regular insight on terrorism, criminal and intelligence related matters. He has extensive experience in understanding as well as investigating complex coordinated attacks. Frankel led several FBI field divisions as the Special Agent In-Charge.*

The CEO, C-Suite and Board all have a much higher potential for being held liable, both personally and corporately, if they don't take the required due diligence and reasonable steps to make sure that the firm is protected from cyber security actors. That wasn't always the case.

Nicole Della Ragione *is an Associate at Ruskin Moscou Faltischek, P.C., where she is a member of the firm's Health Law Department, Cyber Security and Data Privacy Practice Group and the White Collar Crime and Investigations Practice Group. Since joining the firm, Della Ragione's practice has focused in the cyber security arena as well as federal and state litigation. She has been engaged in numerous cyber security engagements ranging across industries and of all sizes. Her work includes advising businesses based on their level of cyber-preparedness and conducting risk and threat assessments, incident response planning and more.*

Nicole Della Ragione: Beyond the fiduciary obligations of the C-Suite, we're starting to see regulations take a turn to putting affirmative responsibilities onto the C-Suite. A good example of that is the new New York Department of Financial Services Cyber Security Regulation, which requires a member of senior management to sign a certification to the Superintendent of the Department of Financial Services stating they are in compliance with the law.

There are enforcement provisions in that specific regulation if they lie, or have not done their due diligence to ensure that they're accurately filling out the certification. As with any sort of certification to the government, there are false claims act liability that comes with it. So, not only do we have the standard liability issues due to the fiduciary obligations of the C-Suite, we're now starting to see regulations actually take a turn and put affirmative obligations onto the C-Suite.

Frankel: That's why we're actually seeing, in many organizations that we've dealt with, the Chief Information Security Officer has direct reporting in many instances to the C-Suite itself, and at times to the CEO so they can show that they've taken, at the very least, reasonable steps to handle all cyber security matters.

Skroupa: How do cyber security issues impact leadership ability to fulfill its fiduciary duties?

Frankel: When a breach happens, it really comes down to asking, "Who is charge of handling that breach?" How is the company responding to the breach? Is it an all-encompassing look by the firm to see how it happened? How do they protect against it in the future?

Just letting a breach happen, and then going in and correcting that issue itself is not enough anymore. Relating their fiduciary duty to the firm, they've got to go in and correct that matter, see how it happened, ensure that it never happens again and most likely have a security assessment done by a reputable firm. Then make reasonable efforts to correct the errors that are found. Again, just by delegating this down is not enough anymore.
The CEO and the C-Suite are now going to have be involved in the decision making to make sure that those corrections and the reasonable steps to ensure that cyber security breaches don't happen moving forward.

Della Ragione: We've actually seen in real time now the sorts of problems the C-Suite will run into when they're not kept properly apprised of data breaches that occur at their companies. A good example of that is what's happening over at Equifax right now. We have members of the C-Suite who sold some stock, supposedly without knowledge of the data breach, and now there's security fraud issues and other issues arising out of the accused C-Suite supposedly not knowing about a data breach.

Skroupa: What threat does spear phishing pose to a company, and how large or worrisome is it?

Frankel: What we're seeing is a lot of companies are aware of spear phishing, but it still poses a great threat. In fact, we've seen – in real-time again – how CFOs and CEOs think that they're talking to each other, and in the end they're getting ripped off. We've had one company, that I've just dealt with in the last week, that was

ripped off for hundreds of thousands of dollars because the CFO thought that he was speaking with the CEO, and so the CFO made significant wire transfers.
To be quite frank, there was another company that we dealt with that did the correct protocols and did a two-factor or factor authentication, in other words as soon as the Administrative Assistant got the word to wire some money she called the CEO and asked if she should follow through on that. The CEO didn't know what she was talking about, and told her not to wire any money.

Della Ragione: In our technological time a lot of people have forgotten that the easiest way to prevent a lot of fraud that we're seeing, especially with spear phishing, is really just to pick up the phone. No one seems to want to talk to each other on the phone anymore, which is really only aiding in the increase of these spear phishing attacks, and how successful they are in acquiring money through these types of attacks.

Now we've seen the most effective way to stop a spear phishing attack for some type of wire fraud is for people to pick up the phone and double check. Did you want me to wire $200,000 to this account that we've never wired money to before? It's a quick easy way to stop that type of attack.

Skroupa: What would you both say is the next step for evolving the cyber security landscape?

Frankel: It's bringing the C-Suite fully into cyber security. We do know that cyber security is not the only thing they need to deal with, of course they need to deal with a whole host of corporate matters that the CEO and other members of the C-Suite would normally have to deal with, but now cyber security is one of those matters.
It can't be pushed off or delegated down. As Nicole said on Equifax, it could be in that case or in something else, we're going to see C-Suite individuals across many companies be held both corporately and possibly personally liable for the breaches that have occurred, and we can only see it getting worse.

Della Ragione: Something that is really important that companies are starting to learn is there really is a difference between cyber security and I.T.
Your general I.T. infrastructure, and your general I.T. team usually don't have the capabilities that an expert in cyber security would. So I think it's really important for companies to understand that they may need to have additional cyber security protections in place in addition to the I.T. resources that they may already have.

SKYTOP STRATEGIES

ABOUT SKYTOP STRATEGIES

As the corporate landscape evolves around global, social, environmental and economic change, **Skytop Strategies** works to facilitate discussion around corporate strategy with C-suite leaders, institutional investors, boards of directors, stakeholders, and authoritative NGO/government agencies. Skytop Strategies convenes companies through **live conferences** designed to empower success and longevity within their respective industries and around the global marketplace. We provide a platform for market-moving dialogue by connecting decision makers through actionable exchange, revolutionizing the way 21st century companies create value. Our programs form an arena for experienced professionals to navigate large-scale concepts and implement sustainable, ethical and productive practices. Topics cover shareholder activism, ESG and sustainability, governance and risk, gender equality, and much more. Skytop Strategies also produces **high-quality content** – interviews, newsletters, feature-length articles, etc. in the form of video, online, print and more – to expand the dialog and support the concepts.

Publishing inquiries:

KALEB SMITH
Associate Editor
ksmith@skytopstrategies.com

Media and Marketing inquiries:

PHILLIP LOFASO
Chief Marketing Officer
plofaso@skytopstrategies.com

Speaker inquiries:

MAURA MURPHY
Managing Director, Program Development
mmurphy@skytopstrategies.com

Sponsorship inquiries:

CHRISTOPHER SKROUPA
CEO & Founder
cskroupa@skytopstrategies.com