Information Security – Top Industry Experts Discuss Threats And Challenges

#BakersDozen on High Performance Counsel

HIGH PERFORMANCE COUNSEL

#BakersDozen is a series of interviews with leading professionals in the fields of law, consulting, finance, tech, and more.

About Paul Ferrillo:

Paul Ferrillo is counsel in Weil's Litigation Department, where he focuses on complex securities and business litigation, and internal investigations. He also is part of Weil's Cybersecurity, Data Privacy & Information Management practice, where he focuses primarily on cybersecurity corporate governance issues, and assists clients with governance, disclosure, and regulatory matters relating to their cybersecurity postures and the regulatory requirements which govern them. Mr. Ferrillo regularly counsels clients on cyber-governance best practices (using as a base the NIST cybersecurity framework), third-party vendor due diligence issues, cybersecurity regulatory compliance issues for private equity, hedge funds, and financial institutions that have been promulgated by the SEC, FINRA, the FTC, and the FDIC/OCC, the preparation and practicing of cybersecurity incident response plans, as well as evaluating and procuring cyber-liability insurance to protect against losses suffered by companies as a result of the theft of consumer or personally identifiable information, or as a result of the destruction of servers and corporate infrastructure.

#BakersDozen is a series of interviews with leading professionals in the fields of law, consulting, finance, tech, and more.

About Shawn Tuma:

Shawn Tuma is passionate about serving his clients. He honors the trust they place in him by working hard to achieve their objectives as effectively and efficiently as possible. His integrity, intensity, and drive for excellence have helped him become an internationally recognized attorney and thought-leader in cybersecurity, computer fraud, and data privacy law, areas in which he has practiced for nearly two decades. He is a Partner at Scheef & Stone, LLP and General Counsel and Director for the Cyber Future Foundation. Shawn frequently assists clients with cybersecurity and data breach related incidents, both as cyber insurance panel counsel and direct engagements. For proactive companies, an ideal role for him is to serve as a member of their team as outside cybersecurity counsel to help them prepare for and minimize the risks of doing business in today's cyber risk-laden business world. Then, if a problem does arise, he is there to guide them through resolving those issues as well. He has worked his entire career as both a cyber lawyer and a complex business trial lawyer, a combination of experience that equips him with unique skills for helping businesses assess, avoid, and resolve problems in a very expeditious manner.

#BakersDozen is a series of interviews with leading professionals in the fields of law, consulting, finance, tech, and more.

About Chuck Brooks:

Chuck Brooks is President of Brooks Consulting International. LinkedIn named Chuck as one of "The Top 5 Tech People to Follow on LinkedIn" out of their 500 million members. He has published more than 150 articles and blogs on cybersecurity and technology issues. In both 2017 and 2016, he was named "Cybersecurity Marketer of the Year by the Cybersecurity Excellence Awards. Chuck's professional industry affiliations include being the Chairman of CompTIA's New and Emerging Technology Committee, and as a member of The AFCEA Cybersecurity Committee. In government, Chuck has served at The Department of Homeland Security (DHS) as the first Legislative Director of The Science & Technology Directorate at the Department of Homeland Security. He served as a top Advisor to the late Senator Arlen Specter on Capitol Hill covering security and technology issues on Capitol Hill. In academia, Chuck was an Adjunct Faculty Member at Johns Hopkins University where he taught a graduate course on homeland security for two years. He has an MA in International relations from the University of Chicago, a BA in Political Science from DePauw University, and a Certificate in International Law from The Hague Academy of International Law.

AN INTERVIEW WITH CYBERSECURITY LEGAL EXPERTS PAUL FERRILLO, ESQ. AND SHAWN TUMA, ESQ.

By Chuck Brooks

Chuck: I am pleased to interview two the best legal minds in the cybersecurity world, Paul Ferrillo, Esq. and Shawn Tuma, Esq. about the threats, challenges and trends in the connected world. Both Paul and Shawn are widely published on cyber risk management, regulatory, and governance topics of special interest to the legal community. They also have been featured speakers at numerous events and conference, including "Artificial Intelligence In The Legal Realm," highlighted in the photo above.

Cyber breaches have exponentially victimized among corporations, organizations, firms, agencies, and individuals in the last few years. Clearly, the threat is growing more sophisticated and prevalent. As leading members of the legal community, what do you see as the biggest challenges in addressing the threat for your clients?

Paul and Shawn:

1. Cyber is not a stationary target, but is constantly evolving in many ways. Threats move and change constantly as bad actors find new means for attacking, new targets to attack, and new ways to monetize their successes. In 2014, the trend was stealing and selling payment card data. In 2015 and much of 2016, it was healthcare data. In 2016, we began to see more ransomware used for extortion, which has increased substantially in 2017. Now we are seeing more attackers using not only encryption of networks through ransomware as a basis for extortion, but also the exfiltration of sensitive data and then threatening to expose that data publicly unless an extortion demand is paid. They are becoming more aggressive and are now layering these different attacks, such as with gain access into an environment and covertly exfiltrating information for sale or extortion and then, as a parting gift, leaving ransomware to encrypt the network, promising to decrypt in exchange for the payment of another ransom. Finally, we are seeing them build on successful attack tools and techniques and modifying them as they go to make them even more effective, such as we saw when Petya moved away from Wannacry ransomware and towards a destructive wiperware attack. Clients simply do not understand and refuse to accept that cyber risk is not going away and there is no one time fix – it is now a way of life and just as the bad guys are continuous with their attacks and are evolving in how they do so, clients must be continuous in their defenses and must continuously reassess and evolve how they are protecting themselves.

2. The "we are not a target" response from clients – clients must begin to understand that if they have data, they are a target, and everybody has data. And with the rise in ransomware there is a new twist, even for clients who do not deal in or otherwise have sensitive data: attackers use ransomware to encrypt their network and deny them access to their entire computer network and all of their data, effectively sending their business back into the Stone Age. Recent attacks showed how attackers show no shame switching industry verticals constantly. Whatever works is repeated. What doesn't work is abandoned for something more profitable. Also the CISO refrain of "oh, we are fine, we have been doing things this way for 5 years." If you hear this refrain you absolutely know things are not fine.

3. Vendor BS – the most concerning. Many vendors fixed on proven revenue streams rather than what is best for the client. For instance, 100% of all successful attacks bypass firewalls. Shouldn't that be a red flag? Shouldn't the conversation move to machine learning solutions? Well of course it should, but sometimes it doesn't or sometimes it doesn't until the client has already been breached.

Chuck: Should anyone formally involved in the world of regulation and compliance be required to have cyber expertise in conjunction with their advisory roles to clients and to the C-Suite?

Paul and Shawn: We find and see that nearly all companies are regulated by at least one regulatory agency or state regulator. Many, like financial institutions, investment banks and commercial banks could be regulated by "several" regulators at one time. Since cybersecurity touches every facet of these business, if you don't have cyber experience you can't be an effective or trusted advocate.

Chuck: GDPR is being enacted in May by the European Union. The GDPR expands the territorial scope of European data protection legislation to make it applicable to non-EU organizations offering goods or services to data subjects in the EU. What are your thoughts on the implications of American and global companies doing business with the EU after May?

Paul and Shawn: For many institutions who might not be familiar with the global consequences of a cyberattack, the GDPR can truly be seen to be a game changer. Especially for American institutions that might have been cybersecurity "centric" but not "privacy centric". There are also many differences in "practice" between American firms (who are generally well schooled in incident response and disclosure issues) and EU firms almost never had to deal with these issues. The time and expense involved with a true GDPR shift will be sizable and some don't have the money or time to fully enact. And if there is a material breach, god help the company that does not disclose the issue to regulators within 72 hours.

Chuck: I am very happy to share that I work closely with the both of you and also Kenneth Holley, George Platsis, Christophe Veltos, and George Thomas, Jr. as part of a unique cyber-education group called #Cyberavengers. In fact, High Performance Counsel has recently published the #Cyberavengers playbook for its readers to download. Can you both describe the vision and mission and why the legal community in particular should be aware of the #Cyberavengers gratis thought leadership offerings?

Paul and Shawn: The #Cyberavengers were created jointly between our love of the old Marvel comic book series, the Avengers, and our desire to help this country deal with what we thought were major disconnects between hype and fact, and between illusion and reality. Americans also suffer greatly from vendor overload (as we have noted above) along with

"tech speak" and techno-babble which muffles and garbles messages. The Cyberavengers have pledged to change the present cyber paradigm of major breaches, and to avenge those actors and countries who attempt to (and often succeed) in hurting this country and stealing its valuable intellectual property. We do our jobs out of love for our country, or states and our communities. We feel we are uniquely suited to help this country through what are proving to be difficult cyber times.

Welcome to

HIGH PERFORMANCE COUNSEL

High Performance Counsel provides a valuable sounding board for legal sector leadership on the issues and opportunities facing the legal sector in the next decade. We call on a diverse spectrum of thought-leaders to share their perspective on what works, what doesn't and where it's all headed. Join us.

Learn more