Themes and Take-aways from May 23rd CFO Leadership Council event on Impending Cybersecurity Threats and Practical Steps to Mitigate Risks

"If you don't walk out of here with anything else, take this (piece of advice) with you. It is not well recognized and understood that Email Business Compromise/Spear-Phishing/Whaling is 20 Times more prevalent (than any other threat)." a panelist stressed and imparted to the CFO audience. He continued by stating that the hundreds of millions of losses suffered by US businesses, (in New Jersey, millions reported losses daily caused by this threat alone) can in fact be prevented. The internet crime report for 2017 released and published by the FBI last week suggest US businesses were impacted by an estimated$600 million in monetary losses caused by email business compromise. And yet what is frustrating is that companies of all sizes are not taking to heart that Cybersecurity Risk is not just an IT or a CISO risk. It is a ***business risk*** that requires C-Suite attention and focus. *this risk can be easily and inexpensively mitigated* in comparison to vast sums of technology investment made to secure systems).

About the Panel Event

Real-world insights, impending threats and practical tips to mitigate risks were discussed with high energy and passion by the panelist group led by moderator, Paul Rohmeyer, Professor of Industry at Stevens Institute of Technology School of Business at last week's CFO Leadership Council hosted event. The illustrious speakers included FBI Newark Division's Supervisory Special Agent and co-chair of the National Advisory Committee for the FBI Director's Office, Brendan Goodwin, Regional Cyber Director for Arthur Gallagher's Northeast region and Mark Snodgrass, Managing Director for Arete Advisors (Areté), NJ-based technology and management consultancy.

The New Jersey CFO Leadership Council hosted event is sponsored by CBIZ, KPMG, Oracle, Capital One Bank, Arthur J. Gallagher and many other premium companies. Angela Tise, the Northeast Regional Director of the CFO Leadership council provided a warm welcome and informed that the event delivered on May 23rd, 2018 was in fact the last in-person (NJ CLC) event for the season. It may be the last event until September, it nonetheless delivered a powerful and informative message, timely and relevant for the CFO audience. The 90-minute dialogue was packed with rich war stories, entertaining anecdotes, empirical statistics, pertinent information about current cybersecurity affairs, real-world lessons learned and practical tips that CFOs could take to mitigate risks. The session was immensely engaging. Not surprising, attendees were glued to the panelists instead of their smartphones as you commonly see at such events. A great testimony to the relevant content the panelists brought to a critical stakeholder group typically less concerned with cybersecurity risks - risks that are often still misconstrued to be mostly IT risks and therefor the responsibility of the CISO (Chief Information

Security Officer) and IT department. A complimentary Cybersecurity Risk Planning and Mitigation Guide designed for CFOs, courtesy of CBIZ, Inc (Risk Advisory) and Arete Advisors (Cybersecurity & Technology Practice) and a two-page article on Spear-Phishing and Whaling were also handed out at the event.

Summary of Take-Aways from the Panel Discussion

What can be surmised from the rich dialogue as key take-aways for CFOs? We have organized the information in themes: Cybersecurity Threat Environment – top threats to be concerned about; Emerging or Leading-Edge Technologies; and, Practical Steps to Mitigate Risks. We have also provided lessons learned from a real-world case study at the end of this article.

This photo is sourced from Glassdoor.com KPMG sponsored the venue of this event but bears no responsibility for this article.

Cybersecurity Threat Environment – What are the biggest threats?

The panel agreed that the rising severity of impact (disruption to business and operations), increasing occurrences and the magnitude of monetary losses are considerations for increasing scrutiny from executive management. Although in this session, it is impossible to discuss all of the prominent and emerging threats, they concur that few items listed below are the ones that CFOs should pay immediate attention to. The list is far from exhaustive. The panelists urge CFOs to keep apprised of the rapidly evolving cybersecurity landscape and continue to develop knowledge of other threats and risks that their businesses should evaluate and potentially act upon. **Advanced Persistent Threat (APT)**

APTs are highly sophisticated attacks perpetrated by sophisticated (often foreign) adversaries to steal intellectual property, or customer/client data from US companies. Almost any business whose crown jewels are its intangible assets such as proprietary technology design, patented processes and trade secrets are a potential victim of such attacks irrespective of the company's size or maturity (start-ups or established). Companies with potentially high value intellectual property range across industries, from technology firms to pharmaceuticals, medical equipment suppliers, entertainment/media to manufacturing, biolabs, food packaging, financial services and distribution. (Reference the statistics for SMBs and large companies in the War Against Breaches article[1] . In addition, client or customer lists are often a target, with the data being sold on the "dark web".

- **Email Business Compromise/Spear-Phishing/Whaling**
  It is a salient point, not well understood, that email business compromise is 20 times more prevalent than any other threat because the economic and financial losses suffered by US companies and individuals (as a result of cyberattacks) are estimated to be more than $600 million in 2017. The message about severity of this risk was reiterated by the examples provided of daily losses suffered by US businesses where $8.8 million and $600,000 were lost just weeks ago and one day before the event respectively, each in a single transaction caused by this type of attack. Even the most sophisticated companies in America are being victimized. A panelist informed us that 10% of Fortune 500 employees' login credentials have been compromised. He suggests that, "You can assume that your credentials have been compromised" and that precaution and additional controls should be

[1] https://www.areteadvisorsltd.com/single-post/2017/08/31/Winning-the-war-against-data-breaches

taken to ensure emails from the C-suite are personally verified orally before transmitting funds and payments requested by the email requestor. C-suite members are specifically targeted by criminals, and it cannot be stressed enough that these criminals are highly sophisticated and could have stolen credentials months or years before the attack. They monitor and "watch" their targeted users' online behavior and then impersonate that user to conduct their attack. The panel shared an important piece of advice - if changes were made to any payment instruction, the changes should be verified through a second channel (e.g. a telephone call/text… but be aware that these sophisticated criminals can impersonate targeted individuals and steal their telephone identity as well). You should verify through a second authority for the payment or transaction, such as the Treasurer, COO, General Counsel and equivalent depending on your organization's policy.

- **Data Exfiltration and Data Theft by Valued, Disgruntled and Terminated Employees and Contractors Alike**
  Among the biggest threats is your most trusted employees and contractors. Numerous accounts have been told about disgruntled and terminated[2] employees stealing valuable information in retaliation. More than 80% of terminated employees reportedly admitted to taking intellectual property from employers when they left. Employee (insider) data theft [3] is on the rise. Within a short span from 2009 to 2015, the insider theft rate grew by 25%. In 2018, it is predicted to get worse.

- **Ransomware**
  1,800 ransomware attacks were reported last year by the Internet Crime Report. (reference article, "Latest Internet Crime Report Released – IC3 says losses exceeded $1.4 Billion in 2017 from https://www.areteadvisorsltd.com/cfolceventmaterials). Ransomware continues to be a threat even if the monetary losses are not as significant when compared with email compromises discussed before.

Emerging or Leading-Edge Technologies to improve your security posture and capabilities

Mark, whose specialty is next-generation technology and leading-edge tools was asked by Paul to provide some examples of technologies CFOs should consider to either improve their security capabilities or lower their security Total Cost of Ownership (TCO) without compromising security posture.

- **Security as a Service**

  The most important piece of advice that CFOs are interested in, by way of technology, was explained by Mark to be security-as-a-service. He stated that the CISOs interest is to develop "defense in depth" to improve the security posture. Defense in depth however, traditionally requires heavy capital investment in several different types of security appliances. To reduce cost significantly while still maintaining or improving their security capabilities, CFOs now have the option of asking their CISOs and CTOs to explore using a security-as-a-service instead. Cloud sandboxing, URL filtering, data loss prevention, firewalls and proxy servers are examples of the types of services offered. By purchasing these solutions as a service, CFOs can avoid expensive hardware capital and maintenance costs.

[2] https://intelligentid.com/data-theft-fired-employees-rise/
[3] https://www.centerpointit.com/data-theft-by-employees/

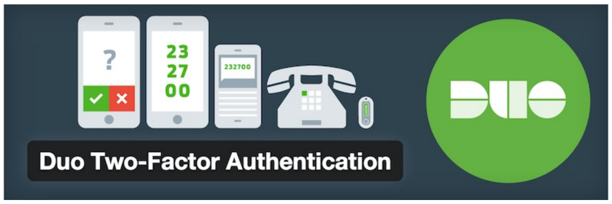
- **Cloud-based Security Services (Deception as a Service, Zscaler Internet Access)**

  Deception-as-a-service (DaaS) creates "honeypots" that lure adversaries, which can then be tripwires for a breach in progress. If any of the honeypots (and there would be many) are accessed, it is a sure indication that a firm has been compromised. DaaS is an adjunct to existing defenses. Zscaler Internet Access is a Cloud Service designed to protect users from the Internet, and to prevent them doing things that would jeopardize your firms' data or reputation. It is a Cloud-based service, with the benefit of the "Cloud Effect", where any malware detected anywhere by any subscriber can be fingerprinted, with all subscribers benefitting from the first detection.

- **User-behavioral analytics tools (Ex: Varonis, DB Networks)**

  He further explained that user-behavioral analytics tools are designed to detect anomalous user behavior, where a user who commonly, for instance, accesses payroll information but begins to also access financial and accounts payable systems. The system will alert and notify your organization rapidly and in a timely manner. For database servers, and new connections from people or application servers can similarly be detected, and management notified in real time.

- **Two-factor authentication Tools (Ex: Duo, TokenOne)** – are necessary to protect sensitive systems with an additional authentication factor in addition to a password. The benefit is that even if the password is compromised, a second independent factor is needed to access the sensitive system. These new style two-factor authentication systems typically deliver the second factor through a smartphone application and improves security against hacked user credentials.



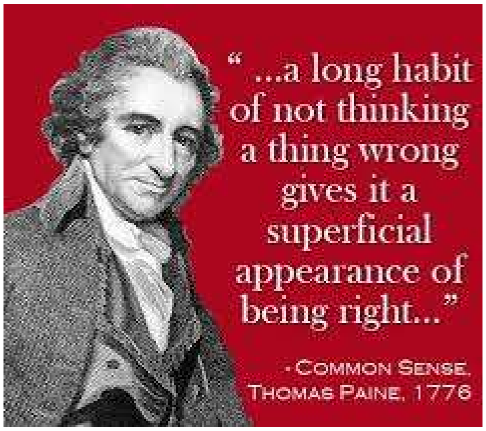
- **Software-defined Perimeter (SDP, a replacement for VPNs, which have been an attack vector for attacks such as the Target stores breach) such as Zscaler Private Access**

  The SDP provides access to a specific application via a secured tunnel connection, instead of a full network connection, as used by VPNs. This prevents lateral movement by attackers once they're inside your network. By preventing lateral movement, any breach that does occur will be limited to the specific system that was attacked, instead of all systems in the company. This is particularly important to decrease the chance of an attack on your company's critical systems such as treasury and core business systems, particularly if the attacker infiltrated your company's systems via a remote user device such as a smartphone or tablet connected to your company's business applications.

- **Privileged Access**

  Privileged access is not new, but it was explained that there are new robust tools that deploy user behavioral analytics and real-time notification of unusual behavior by your administrators entrusted with keys to your crown jewel systems. These new capabilities are key to not just detecting suspicious privileged user behavior but also notifying key officers in your organization in real-time so that corrective action can be taken quickly.

Practical Steps to Mitigate Risks – How should CFOs prepare for this?


"...a long habit of not thinking a thing wrong gives it a superficial appearance of being right..."
- Common Sense, Thomas Paine, 1776

Understand your organization's cybersecurity risks and your current capabilities

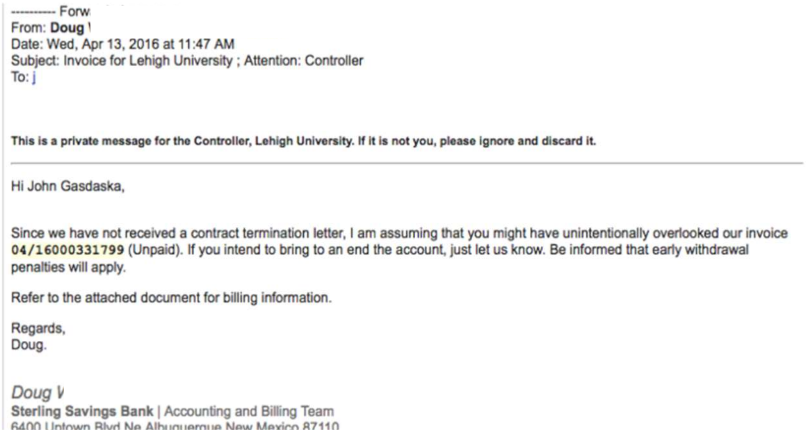
The first step CFOs could take is rudimentary but essential. Evaluate your cybersecurity risks in collaboration with your CISO and CTO. If you have a small business, and you do not yet have a CISO or CTO, engage your entire Executive Team, and enlist interim CISO (insource) assistance. Understand what your biggest risks are (highest likelihood, highest impact, and lowest likelihood, highest impact), what your current capabilities and controls are to address those risks and identify the biggest gaps in your security capability and external/internal specialized cybersecurity skillsets needs.

Awareness

Create an organization-wide vigilance and awareness about the threat of email business compromise, spear-phishing and whaling. See exhibits of real-world examples below where emails were targeted (spear-phishing) by cyber criminals to individuals with valuable login credentials or signature signing authority. These emails appear to untrained employees and executives alike to be legitimate emails because of the sophistication of the attacks. Thousands of incidents have occurred, at large Fortune 500 companies and small mom-and-pop shops alike, where targeted employees and executives were tricked into releasing payments and millions of dollars to what they thought were legitimate requests made by their CEOs, CFOs, Accountants and other senior ranking officers. When these emails are received, many times employees and executives are so busy that they seldom have time to doubt the validity of those requests for payment transfers, wire transfers, and other financial transactions. Create awareness by developing and cascading well-crafted communications throughout the organization to raise awareness and assess the effectiveness of the communications.

Exhibits of Real-World Examples of Spear-Phishing/Whaling (Names may have been fictionalized or redacted for confidentiality purposes)

11. Sent "From" Recipient's Bank



---------- Forw
From: **Doug** \
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

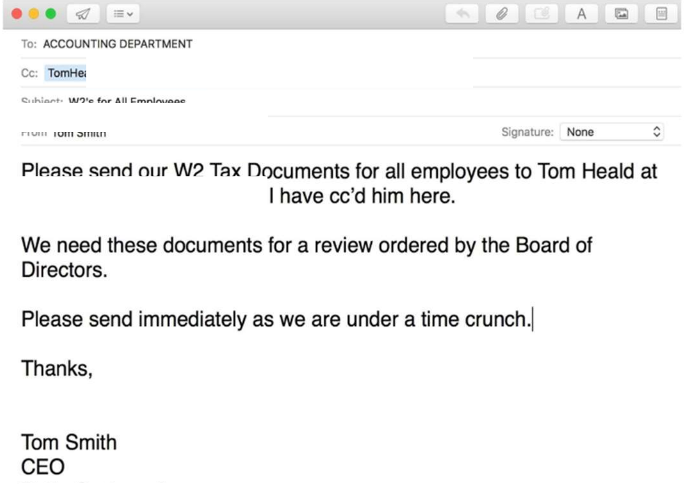
Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice 04/16000331799 (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

Refer to the attached document for billing information.

Regards,
Doug.

Doug V
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne Albuquerque New Mexico 87110

17. Sent to Controller "From" Their CEO (Also CCing Their Accountant)



To: ACCOUNTING DEPARTMENT
Cc: TomHea
Subject: W2's for All Employees
From: Tom Smith
Signature: None

Please send our W2 Tax Documents for all employees to Tom Heald at
I have cc'd him here.

We need these documents for a review ordered by the Board of Directors.

Please send immediately as we are under a time crunch.

Thanks,

Tom Smith
CEO

Practical Steps to Mitigate Risks (con't)

Training is essential at all levels of the organization to improve an organization's security resiliency

Education/Training

All panelists concur and reinforced the need for CFOs to urge their organizations to provide training and education to their C-suite and employees as part of the risk mitigating strategy. Relatively inexpensive, panelists reiterated the notion that awareness, training and education are an essential and powerful mechanism to adequately arm employees and executives who ought to be seen as the first line of defense against cybersecurity attacks, to alert authorized officers of the company or their CISOs of any suspicious activities. The Audience was encouraged to view the risk as an ***Enterprise Risk***, and for their C-Suite and executives to be educated to take an active role in managing this risk. As stated in the two-page hand out that was distributed at the event on "Tips for CFOs to Mitigate Against Spear-Phishing and Whaling Risks"[4], culture and fostering the right attitude about security defense is as important as CISOs taking measures to institute the right cybersecurity policy and CTOs implementing the appropriate security technology – to fight against cyber-crime.

Enlist the assistance of external and professional experts to provide inexpensive training and education to employees and executives on how to recognize business email threats, spear-phishing and whaling. Professional training simulates these attacks in a way that organizations' training and HR departments are not skilled and equipped to do. Classroom or online self-paced training alone will do little to impart the knowledge needed for employees to adequately learn how to recognize an attack and what to do in the event of such an attack.

Basic Controls

Before investing in new technology or cybersecurity programs, conduct a cybersecurity risk assessment to identify your organization's biggest risks, your current security capability and the gaps in your current capabilities to address those risks. Also, evaluate whether your organization has in place basic and effective cybersecurity controls. Adequate password security, patch management processes, risk management governance and well-defined security policies that are applied effectively are examples of some basic controls.

Timeliness is key to detection, preparation and response

Timeliness in both Detection, Preparation and Response

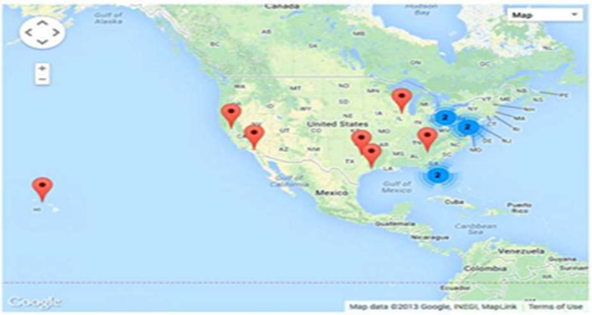
The panelists stressed the importance of timeliness in your organization's ability to execute your incident response plan (IRP) quickly. In many cases, if cyber criminals are not reported and caught within 72 hours, the likelihood of recovering funds are almost impossible. It is important to note that law enforcement agencies are not responsible for executing your IRP and recovering lost funds. However, they can be an important participant and collaborator in the event of a major incident. Your organization should therefore seek to incorporate communications, protocols

[4] Tips for CFOs to Mitigate against Spear-Phishing and Whaling Cyber Attacks from https://www.areteadvisorsltd.com/cfolceventmaterials

and engagement with law enforcement stakeholders as part of your IRP planning and development process. Standard operating procedures should be very clearly developed and simulated to prepare for a cyberattack (be it a ransomware, phishing or APT) because during the attack, there is this "fog of war" chaos. With trained employees and clear protocols to follow, you can react with discipline and timeliness to stop the criminal from causing more damage than has already occurred, and you can also investigate the crime quickly.

Distributed Control

Next to timeliness, they also stressed the need to ensure your organization's distributed environment be properly secured on all devices, across all business units and internet edges (the outer perimeter of an organization's network of systems). If a user's remote device is infected, and this device is connected to the company's network of systems, core systems or crown jewels, the entire organization of users and systems could become infected rapidly. Salespersons and highly mobile contractors, employees and executives frequently inadvertently and unknowingly expose and/or increase a company's security risk.



Organizations with distributed workforce, locations and/or facilities must ensure controls are operating effectively on all devices, across business units and internet edges.

Affordable Best-in-Class Tools to Improve your Cybersecurity Posture and Capabilities

Leverage newer technologies with cloud capabilities, security-as-a-service and user behavioral analytics. Mark explained that in his consulting for SMBs with as few users as25 up to hundreds of users, he discovered that many are not aware that the accessibility these technologies have leveled the playing field for small and large businesses. A small company with $50 to $200 million in revenues can equally afford these tools that large companies like United Airlines have implemented. These tools run the gamut from Duo (for two-factor authentication) to Zscaler (for user device internet security). They can be procured for pennies to dollars per user, and not millions as perceived by many SMBs.

Tip: Reference the Cybersecurity Risk Planning and Mitigation guide for CFOs[5] for additional inexpensive practical tips and avoid common pitfalls (page 4)

Cyber and Social Engineering Insurance

One of the panelists whose specialty is to help companies make good cybersecurity insurance investment advises CFOs to evaluate the adequacy of their current cybersecurity insurance coverage and understand what is covered and not covered. He also explains that to add a social engineering rider clause to their existing business insurance policy would probably cost just 10% more in premium to mitigate against some of the financial risk, a small cost for peace of mind.

Last summer, one of the country's largest global law firms (which had previous to the incident touted its expertise on cybersecurity) had a rude awakening when their sensitive client files were held ransom for millions of dollars. Client facing work including court trials were majorly disrupted because the company had to shut down even its most basic operations like email. The prominent firm lost a full day of phone use, 6 days of business email access, and weeks of inaccessible documents and archived emails. To add salt to the wound, the company discovered that its insurance policy covered some of the losses but didn't cover nearly enough. In a similar situation, another local Rhode Island law firm who lost $700,000 in billable work because it was shut-down for 3 months due to a ransomware attack was equally disappointed to learn, due to lack of understanding of what was covered and the amount of coverage they had, that their insurance company declined the firm's cyber insurance claims. Law firms' sensitive client data are these firms

[5] https://www.areteadvisorsltd.com/cfolceventmaterials

crown jewels and a treasure trove for hackers. Law firms are not the only service firm or industry with sensitive client data. Diligently take stock and evaluate your crown jewels and understand where they reside - and how well protected they are. Cyber insurance, if properly evaluated and purchased can be used to complement other risk mitigating strategies to lower an organization's risk exposure.

Simulation and Preparation to Respond to Incidents/Breaches/Attacks

Inclusion is encouraged in the preparation and simulation exercises to plan, prepare and be ready for how to respond to an attack. Cultivate a culture and environment that fosters open communications and the ability for employees to properly identify and escalate to the C-Suite and CISO's matters that may pose a threat to your organization. Our panelist also promotes leveraging your existing insurance brokers to learn what options are available that you may not already be aware of. See Risk Guide for additional guidance. Your organization should seek to understand what your insurance broker's notification and communication requirements are to trigger a cybersecurity insurance claim due to a breach. He also explained that when you do make the call to your insurance broker in the event of a breach, make sure you are talking to the right person. A breach coach is commonly an attorney that a claims adjuster may bring in as the quarterback to coach you through the discovery and investigation process. The breach coach would normally hire a forensics firm to conduct the investigation in a manner that would protect the confidentiality of the communications related to the breach.

Cloud Security and Cloud Storage/Backup

While this topic was not discussed in great detail due to time constraints, several of the attendees raised the question of cloud storage and the importance of ensuring proper cloud security with a panelist after the session. For this reason, we thought it might be worthy to repeat in this article to benefit the broader audience.   Cloud storage and backing up sensitive data to the cloud is a more common and accepted best practice today than it was, say, only a few years ago. Having said that, a panelist cautions that organizations need to remember that cloud service providers like AWS (Amazon Web Services, Azure, Alibaba, etc.) still require businesses and data owners to take responsibility for ensuring that the proper security frameworks and controls are configured and tested for operational effectiveness to secure their data. The data is as safe as you could secure it on-premise. However, you must take measures to follow the vendor's recommended security framework, and or enlist the assistance of external consultants specializing in cloud security to implement, test, monitor and remediate proper controls. It should also be recognized however that running backups to the Cloud may be more secure and resilient than on-premise backups, as there is no longer the requirement to transport physical tapes to a secure location.

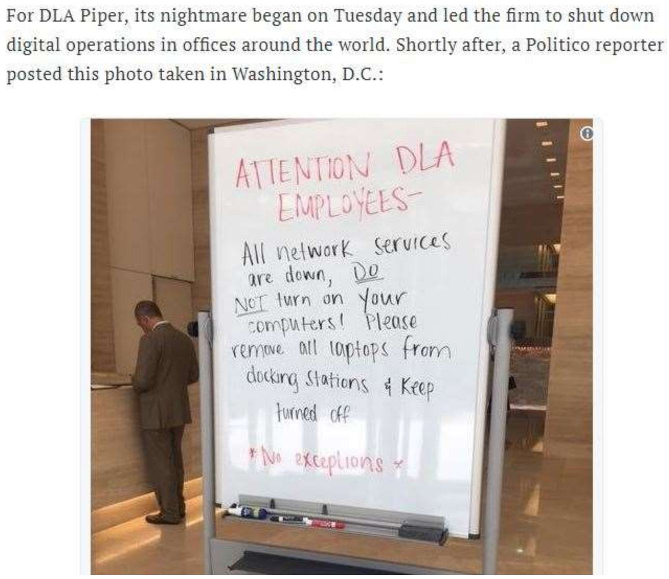
GDPR Compliance

Lastly, panelists reminded the attendees that GDPR requirements apply to US companies, and measures should be taken to make sure those requirements are properly understood and addressed. GDPR is effective May 25th, 2018. *Refer to Risk Guide for more details.*

Lessons Learned from a Real-Word Case Study

Not surprising, the lessons learned from DLA Piper[6] are the same ones that the panelists tried to drive home:

The following is an actual photo of incident reported by Fortune



For DLA Piper, its nightmare began on Tuesday and led the firm to shut down digital operations in offices around the world. Shortly after, a Politico reporter posted this photo taken in Washington, D.C.:

ATTENTION DLA EMPLOYEES-
All network services are down, DO NOT turn on your computers! Please remove all laptops from docking stations & Keep turned off
No exceptions

- Define and have in place an Incident Response Plan (IRP).
  Reference CFO Quick Guide for Cybersecurity Risk Planning and Mitigation[7].

- Don't just have a robust IRP, make sure all the actors in your IRP are trained and communicated to, and everyone knows what their role and responsibilities are

- Simulate your IRP until it becomes as strong as "muscle memory"

- Take measures to ensure the effectiveness of your basic cybersecurity risk mitigation controls: Patch your systems, and isolate those you cannot

- Protect end-points and devices organization-wide, particularly if your organization is geographically dispersed and you have a distributed workforce, facilities, offices, plants, and factories. Secure all machines, including those of employees' and contingent staff and third-party providers who are connected to your systems.

- Ensure there is a 3-2-1 backup plan for your most critical assets/crown jewels (ex: sensitive customer data, intellectual property such as patented processes and proprietary technology/software design and codes).

Editor's Conclusion

Empirical[8] evidence from multiple sources show that among the top cybersecurity threats, the risks of these threats can be significantly lowered and mitigated through prudent and collaborative management among C-suite members and their CISOs and CTOs. It is when the risks are considered by an organization to be solely an IT or CISO's risk and responsibility that the organization increases its own risk exposure due to lack of coordinated, appropriate and meaningful measures and strategic approach to combatting these risks. As with all the biggest threats and themes discussed earlier, data breaches caused by hackers remain a dominant cyber threat to US businesses and businesses worldwide. It is also important to recognize that sensitive data leakages caused by employees' and/or third-party providers' misconfigured security controls for cloud services, faulty backups, and poor cloud storage controls are also

[6] http://fortune.com/2017/06/29/dla-piper-cyber-attack/
[7] https://www.areteadvisorsltd.com/cfolceventmaterials
[8] https://www.areteadvisorsltd.com/single-post/2017/08/31/Winning-the-war-against-data-breaches

rising at an alarming rate as businesses take to cloud but fail to institute proper governance. Big name[9] companies such as Deloitte, Dow Jones, Accenture, Booz Allen Hamilton and Verizon, and Republican Party Data Analytics'[10] firm have all suffered world-stage embarrassments, reputational and financial risks because of improper cloud security controls and/or configurations while using Amazon (Cloud) Web Services (AWS) and equivalent. These are companies with massive financial and human resource muscle. The point is no company, irrespective of its size is immune to cybersecurity threats[11]. The most important thing to remember if you are using Cloud Services is that there are responsibilities for both the Cloud Service Provider and the Cloud consumer, and the demarcation line for those responsibilities needs to be clearly understood. Not deploying Cloud because of the risks is not an option either as to remain competitive and cost-efficient, companies find Cloud is not a hype but in fact a table stakes or competitive enabler.

Additional Resources
For additional complimentary reference materials and white papers on common sense (cybersecurity) IT Security Controls and Measures, EU's GDPR Requirements for US companies and How to Prevent Data Breaches/Data Exfiltration, go to https://www.areteadvisorsltd.com/cybersecurityresources or contact the following panelists and resource contact persons:

Brendan Goodwin, Regional Cyber Director, Northeast, brendan_goodwin@ajg.com, Arthur J. Gallagher & Co. – CFL LC Member and Sponsor
Mike Doyle, Acting Assistant Special Agent in Charge of the Newark Division, FBI, email intentionally omitted by request. Contact Resource Contact Persons below to contact this person.
Mark Snodgrass, Managing Director, Technology and Cybersecurity Practice, Arete Advisors - ms@areteadvisorsltd.com
Paul Rohmeyer, Professor, Stevens Institute of Technology School of Business (***Moderator***) - rohmeyer@tbv-group.com

[9] https://businessinsights.bitdefender.com/worst-amazon-breaches
[10] https://www.csoonline.com/article/3201201/security/rnc-data-analytics-firm-exposes-voting-records-on-198-million-americans.html
[11] https://www.areteadvisorsltd.com/single-post/2017/08/31/Winning-the-war-against-data-breaches

Editor
This article is written by Areté Advisors' editorial team.

Collaborators
This publication is produced in collaboration with the following event sponsors:
CBIZ, Inc.
The CFO Leadership Council

Due to agency and company compliance and time constraints, reference to specific panelists were limited to contributors who received approval from their respective organizations prior to the publication of this article.

Disclaimer
This publication does not constitute professional advice and you should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Arete Advisors LLC and its collaborators listed above do not and shall not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Resource Contact Persons

If you missed the registered event and would like a debrief, copies or additional copies of the materials (Ex: Cybersecurity Risk Guide for CFOs) handed out:

Karyn Egeland, kegeland@cbiz.com, CBIZ, Inc., CFO LC Member and Sponsor

Debbie Lindner, debbie@cfolc.com, CFO LC., Marketing Director, Northeast Chapter

Lilian Snodgrass, ls@areteadvisorsltd.com, Managing Director, Arete Advisors, event Risk Guide and Article Sponsor

TheCFO Leadership Council

(E) debbie@cfolc.com
(P) 516.659.7640

About The New Jersey CFO Leadership Council

Serving to empower CFOs since the fall of 2015, our New Jersey chapter is made up of senior financial executives from a wide range of industries including healthcare, manufacturing, technology, finance, and professional services. Specifically designed by CFOs and for CFOs, we are dedicated to developing strong leadership and relationships at all professional levels, from controller to CFO. Our programs include interactive panel discussions where speakers, as well as members, share advice, information, and best practices on the issues faced by today's CFOs. Our most popular topics have included cash management strategies, post M&A integration, and employee recruiting and retention strategies.

Website: http://www.cfoleadershipcouncil.com/

CBIZ

(E) kegeland@cbiz.com
(P) (212) 790-5788

About CBIZ

With more than 100 offices and 4,600 associates in major metropolitan areas and suburban cities throughout the U.S. CBIZ (NYSE: CBZ) delivers top-level financial and benefits and insurance services to organizations of all sizes, as well as individual clients, by providing national-caliber expertise combined with highly personalized service delivered at the local level. We are one of the nation's leading accounting providers, employee benefit specialists, risk advisory consulting firms, valuation firms and retirement plan service providers. Our Risk Advisory Services provide cost recovery, cybersecurity, enterprise risk management, General Data Protection Regulation (GDPR), Internal Audit, Sarbanes-Oxley, Vendor Risk Management, Forensic Accounting and Payment Card Industry Compliance solutions and services.

Website: https://www.cbiz.com/risk-advisory-services

areté

(E) contact@
areteadvisorsltd.com
(P) (862) 295-1488

About Arete Advisors (Areté) – *Achieve More* With Less

Arete Advisors (Areté) is a boutique management and technology consulting firm. Based in New Jersey and a proud member of North Jersey Chamber of Commerce, we serve the Tristate area, major US locations and select international markets (India, Africa, UAE). We specialize in strategic planning and development, advanced data analytics (solution-as-a-service, implementation), technology implementation, risk management, governance and compliance, transformational change, cloud and cybersecurity solutions, Lean Six Sigma, process optimization, business process re/engineering, program management support and interim management. Our team of cybersecurity advisors are credentialed to provide consultation and implementation of top Gartner-ranked cybersecurity, cloud and next-generation technology products and tools that utilized software-defined parameters, and AI capabilities.

Website: https://www.areteadvisorsltd.com/cybersecurity