Cybersecurity and IT Security Resiliency Risk Planning and Mitigation Quick Guide for CFOs

TheCFO Leadership Council

areté

CBIZ

This publication is a collaboration between The CFO Leadership Council with CBIZ, Inc. (Risk Advisory Practice) and Arete Advisors (Technology Practice). For more information about this publication, contact the persons below:

The New Jersey CFO Leadership Council

http://www.cfoleadershipcouncil.com/	(E) debbie@cfolc.com	(P) 516-659-7640
https://www.cbiz.com/advisory	(E) kegeland@cbiz.com	(P) 212-790-5788
https://www.areteadvisorsltd.com	(E) ms@areteadvisorsltd.com	(P) 862-295-1488

Cybersecurity and IT Security Resiliency
Risk Planning and Mitigation
Quick Guide for CFOs

Applicable for Med-Sized and Larger Organizations with equal or greater than $200 Million Revenues

01 Understand What's At Risk and Where are your Biggest Risks

Assess, Plan, Mitigate, and Monitor your Security Risks like you would your financial risks

- ❑ When was the last time your organization conducted a comprehensive risk assessment? Conduct IT and Cybersecurity Risk Assessments, at minimum, annually. Regularly monitor and update your risk and mitigation plans if your business has been compromised in recent years
- ❑ Clearly understand the drivers of your business needs, IT security needs and associated risks
- ❑ Identify what regulations and requirements have the greatest impact on your **business** (e.g. HIPAA, GDPR, local, state, federal requirements, data protection, privacy, etc.)
- ❑ Identify your biggest security threats and vulnerabilities. Risk rank, prioritize and focus on the highest and medium risks, highest probability and severity of impact
- ❑ Identify your crown jewels and the location (systems, files, database, cloud/on-prem, servers, etc.) where they reside
- ❑ Determine how well-protected your most sensitive data is

02 Understand Your Current Security Management Capabilities

Assess and identify the gaps in your current state IT security and cybersecurity management capabilities

- ❑ Based on your risk mitigation plan, determine your organization's ability from a people, process, policy, tools and technology capability standpoint, to mitigate the highest and medium risks identified
- ❑ Assess skills, bench strength and capacity
- ❑ Identify policy, process, and procedural gaps. As an example, does your organization have an incident response plan procedure and policy and event escalation procedure in place?
- ❑ Do you have a documented notification plan for key internal (board of directors, C-suite, key leaders and employees) and external stakeholders including customers/donors, federal/state/local law enforcement agencies, your lawyers, regulatory bodies and insurance agencies that you must notify to comply with applicable insurance as well as state, federal and foreign laws – in the event of a reportable incident? Note: Federal and state law enforcement agencies are potential collaborators in investigation of major incidents, and you are encouraged to speak with your respective agencies to understand and coordinate protocols for notification and to assist your organization in the event a major investigation is needed.

Cybersecurity and IT Security Resiliency
Risk Planning and Mitigation
Quick Guide for CFOs

Applicable for Med-Sized and Larger Organizations with equal or greater than $200 Million Revenues

03 Develop Appropriate Strategies

Develop appropriate comprehensive strategies and realistic thoughtful plans to execute risk mitigation plans and address gaps in your IT security capabilities

- ❑ Establish a phased-approach roadmap and program to address risk mitigation requirements and capability gaps
- ❑ Develop a comprehensive strategy that enables your organization to build security resiliency against mounting security challenges and increasingly aggressive cyber attacks and criminals. Have in place:
  - ✓ A holistic strategy that considers all types of security threats (vulnerability mgt, insider data theft, data protection, business application and IT infrastructure security, data loss prevention, physical security, critical assets (e.g. factories, logistics, supply chain distribution network, sensitive client data, etc.) and devices
  - ✓ Clear roles and responsibility for assessing, managing, monitoring and remediating risks
  - ✓ A robust plan to address capability gaps and develop maturity in your Security Operations Center capability or program. Visit https://digitalguardian.com/blog/how-build-security-operations-center-soc-peoples-processes-and-technologies for insights about Building a Security Operations Center
  - ✓ Properly allocate qualified cybersecurity skills and talent. Seek external assistance for specialized skills, difficult to source talent or expensive talent to hire permanently for work that can be done on project-basis
  - ✓ Cybersecurity awareness training and cyberattack prevention education for employees, contractors and executives in addition to skill development programs for IT security staff
  - ✓ Adequately evaluate, plan and budget sufficient funds on an annual basis to invest and develop your in-house security capabilities and to adopt next-generation security technology and tools to defend against sophisticated cybercriminals and to stay current with advanced technologies (machine learning, AI)
- ❑ Leverage and tailor applicable industry acceptable standards and frameworks such as the federal guidelines and National Institute of Standards and Technology (NIST) for improving critical infrastructure security (Visit https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) for your environment

04 Don't Go To It Alone

The challenges and cybersecurity landscape are constantly evolving and rapidly changing. Stay current by attending info-sessions, webinars, roundtables and knowledge exchange sessions. Seek to learn at others' expenses, gain lessons learned and develop real-world insights about use cases, best practices and emerging and next-generation cybersecurity technologies from cybersecurity professionals and technology management consultants.

Cybersecurity and IT Security Resiliency
Risk Planning and Mitigation
Quick Guide for CFOs

Applicable for Med-Sized and Larger Organizations with equal or greater than $200 Million Revenues

05 Avoid Common Pitfalls

Lessons learned from others

- ❑ Communicate and cascade communications throughout the organization about your organization’s security risk plans with key stakeholders across all functions and business units
- ❑ Build business cases to justify financial investments in cybersecurity programs and make informed decisions
- ❑ Engage the C-Suite and Board of Directors in investment decisions and planning (cybersecurity programs) because it is not an IT risk but a top business risk.
- ❑ Proactively collaborate with your CISO (Chief Information Security Officer) and CTO (Chief Technology Officer) to ensure appropriate funding is allocated and investments monitored, measured and managed to adequately prevent and defend against cybercriminals and mitigate against reputational risk and financial losses
- ❑ Users are the weakest link in an organization’s security posture. In addition to training, consider User Behavior Analytics (UBA) and AI/ML techniques to assist in catching anomalous behavior (“Verify, then trust”)
- ❑ Develop, practice and run simulated breaches to develop “muscle memory” response
- ❑ Realize that the number one IT security threat lies in your organization. That’s right. It’s your people. A Federal Agency officer for IT security once said, “CEOs to secretaries, they all peruse websites they should not”. Awareness training and education is necessary to prevent behaviors that could inadvertently harm your network and shut down your business. Tools like Varonis that the Federal Agencies like Defense Logistic Agency uses deploy artificial Intelligence and behavioral analytics. These tools help prevent and mitigate risks of insider threats (internal employees stealing sensitive data).

06 Practical Must-Haves - IT Security Practices

*Important Must-Have Practices You Can Implement **Today**. Many of these are inexpensive to address and can make a difference to your security posture.*

- ❑ 56% of cyberattacks use a method called Phishing. Develop and train your employees and executives on ***Phishing*** (a sophisticated technique used by hackers to trick employees and C-suite to unknowingly give criminals access to your user credentials which are then used to steal data and hold you ransom for money)
- ❑ Implement two-factor authentication tools
- ❑ Begin cultivating a culture where “Security is everyone’s responsibility”. Start this process today.
- ❑ Ensure “Principle of Least Privilege” is rigorously applied, particularly to core systems/systems with sensitive data
- ❑ Conduct penetration testing and vulnerability assessment semi-annually/annually

Cybersecurity and IT Security Resiliency
Risk Planning and Mitigation
Quick Guide for CFOs

Applicable for Med-Sized and Larger Organizations with equal or greater than $200 Million Revenues

07 Data Exfiltration Capability Self-Assessment

Is your organization sufficiently prepared to prevent, defend, detect and contain stealth attacks? Here's one way to find out. How many of these questions can you respond to with confidence if asked by your board of directors or senior management team?

□ How frequently does your organization assess your security risks?

□ Are your risks assessed continuously?

□ Who are your critical data owners? What level of engagement does your IT and security team have with your business data owners? Are they (data owners) involved in key risk identification, planning and mitigation decisions?

□ What mechanisms do you use to properly classify data?

□ On a scale of 1-10, how well protected should your crown jewels be? On a scale of 1-10, how well protected are they currently?

□ What is the gap between where you should be and where we you are today with capabilities and risk mitigation?

□ How well are those gaps being addressed?

□ Do you have a robust roadmap for addressing those gaps and risks?

□ Are those gaps being addressed using the best defense, detection and containment capabilities and technology available?

□ Can you detect stealth attacks?

□ How do you know your systems are infected?

□ How quickly can you detect a system infection?

□ How quickly can you contain an attack?

□ What is your backup plan?

□ Do you have the expertise in-house to do all that is needed to secure our data at the levels needed?

Visit and download the white paper with additional information on this assessment and data exfiltration techniques - https://www.areteadvisorsltd.com/single-post/2017/08/31/Winning-the-war-against-data-breaches

TheCFO Leadership Council

areté

CBIZ

This publication is a collaboration between The CFO Leadership Council with CBIZ, Inc. (Risk Advisory Practice) and Arete Advisors (Technology Practice). For more information about this publication, contact the persons below:

The New Jersey CFO Leadership Council

http://www.cfoleadershipcouncil.com/ (E) debbie@cfolc.com (P) 516-659-7640
https://www.cbiz.com/advisory (E) kegeland@cbiz.com (P) 212-790-5788
https://www.areteadvisorsltd.com/changemanagement (E) ms@areteadvisorsltd.com (P) 862-295-1488

Cybersecurity and IT Security Resiliency
Risk Planning and Mitigation
Quick Guide for CFOs

Applicable for Med-Sized and Larger Organizations with equal or greater than $200 Million Revenues

08 Is your Data Protection Program adequate to mitigate against risks?

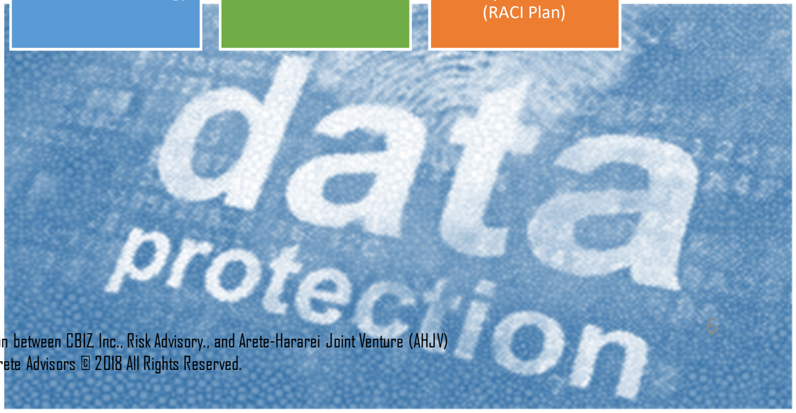
Apply a Holistic Framework for A Robust Data Protection Program to protect sensitive and critical data (assets)

Pillars of a strong and robust data protection program are multi-faceted: from leadership and strong sponsorship to deploying next-gen technologies and having the right people, tools, policies, governance and subject matter expertise, many elements must be considered for your data security program strategy to be effective.

The undertaking to improve a company's data protection capability is complex, the effort for which should not be underestimated and must be approached holistically as a multi-phased program, and not as a one-off project. The consequences of not doing so would result in wasted investment, productivity loss, and a slap-dash data security program that does little to prevent, let alone detect and stop a large-scale infection.

Data Exfiltration Program Framework
Arete Advisors ©2018 All Rights Reserved

Senior Management Sponsorship/Support & Stakeholder Management	Identify and Protect Crown Jewels	Governance (Metrics, Reporting, Accountability)	Employee Training/Awareness
Comprehensive Data Security Program (Prevent, Detect, Contain/Respond)	Prevention Strategy	Standardized Processes/Well-Defined Procedures (e.g. Pre-defined IRP)	Right Mix of People and Expertise (in-house/external)
Next-Gen Technologies (Keep pace with hackers)	Detection Strategy	Policy, Audit and Compliance	Culture Change ("Security is everyone's responsibility")
Risk-Based Assessment and Prioritization Approach	Containment Strategy	Data Classification	Roles & Responsibilities (RACI Plan)



hararei
Edge Solutions Provider

This publication is a joint collaboration between CBIZ Inc., Risk Advisory., and Arete-Hararei Joint Venture (AHJV)
Arete Advisors © 2018 All Rights Reserved.

Cybersecurity and IT Security Resiliency
Risk Planning and Mitigation
Quick Guide for CFOs

Applicable for Med-Sized and Larger Organizations with equal or greater than $200 Million Revenues

09 GDPR Readiness

Are your GDPR regulatory compliance risks sufficiently mitigated?

□ Is your organization prepared and ready to comply with GDPR regulatory requirements by May 25th, 2018?

□ Has your organization conducted a compliance readiness assessment?

□ Have key stakeholders/leaders across the business unit and support functions been informed/educated about GDPR requirements and your compliance program?

□ Have the C-Suite and Board of Directors been educated about your organization's top GDPR risks, and mitigation plans? Have they accepted the risks ranked high and medium for severity of impact and likelihood of occurrence?

□ Do your stakeholders understand all US companies with > 250 employees must comply with GDPR with some minor exceptions for micro and small businesses?

□ Does your C-suite and Board of Directors understand that the non-compliant penalties are as high as 2% of total global revenues, and $10M in fines?

□ Experts have stated EU authorities would have the enforcement powers to audit or penalize non-complying US entities who hold or process customers (data) who are EU citizens and Americans' with EU citizenship although it is unclear how this would materialize. Has your organization validated with high level of confidence that it does not store or process these types of data?

! Visit "Doing Business with EU Citizens and the European Union" under the Section, "Quarterly Cybersecurity Expert Picks" and download GDPR guidelines from https://www.areteadvisorsltd.com/cybersecurityresources

Cybersecurity and IT Security Resiliency
Risk Planning and Mitigation
Quick Guide for CFOs

Applicable for Med-Sized and Larger Organizations with equal or greater than $200 Million Revenues

NOTE

Your Take-Aways from the Panel Discussion

Speakers

Mike Doyle
Supervisory Special Agent
Federal Bureau of Investigation

Brendan Goodwin
Regional Cyber Director - Northeast
Arthur J. Gallagher & Co.

Paul Rohmeyer
Professor
Stevens Institute of Technology
Moderator

Mark Snodgrass
Managing Director
Technology and Cybersecurity Practice
Arete Advisors

Download the electronic (PDF) copy of this guide from https://www.areteadvisorsltd.com/cfolceventmaterials
Password: AreteMay232018

Cybersecurity and IT Security Resiliency
Risk Planning and Mitigation
Quick Guide for CFOs

Applicable for Med-Sized and Larger Organizations with $0.5B+ Revenues

This Publication & Disclaimer
Part of the contents in this publication has been previously published by Arete Advisors and Hararei, Inc. 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, CFO Leadership Council, CBIZ, Inc., Arete Advisors LLC and Hararei, Inc. do 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.

This publication is a collaboration between The CFO Leadership Council with CBIZ, Inc. (Risk Advisory Practice) and Arete Advisors (Technology Practice). For more information about this publication, contact the persons below:

TheCFO Leadership Council

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

(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**.**

CBIZ

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

(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**.**

areté

Website: www.areteadvisorsltd.com

(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, project management, program management support and interim management.

Special thanks to Hararei, Inc. for content contribution.

hararei

Edge Solutions Provider

Website: www.hararei.com

(E) contact@hararei.com
(P) (702) 608 8283 (USA & Global)

About Hararei, Inc

Hararei, Inc. is an international strategic technology service provider and consultancy firm. We specialize in strategic IT planning and development, IT risk assessment, IT transformational change, IT modernization, cloud, cybersecurity, software-defined WAN solutions, SAAS, PAAS, and IAAS. We are also a value-add reseller for a broad range of Gartner-ranked leading and next-generation products including Amazon Web Services (AWS), Varonis, Zscaler, Duo and Silver Peak. Our clients include Federal Agencies such as the Office of Inspector General, SMBs and large corporations.