INTRODUCTION TO REVENUE-CENTRIC CYBERSECURITY

Eclipsing traditional cybersecurity, Revenue-Centric Cybersecurity simultaneously helps organizations (1) mitigate business-threatening cyber risks and (2) increase revenue.

THE GOALS OF REVENUE-CENTRIC CYBERSECURITY

Revenue-Centric Cybersecurity is an innovation that increases profitability by helping organizations invest in only the cyber risk mitigation needed to (1) reduce business-threatening cyber risks to an acceptable level and (2) produce the proof to persuade clients, partners, and strategic buyers that they and their offerings are cybersecure. It represents an important advancement in the evolution of cybersecurity[i] – as this Figure 1 introduces:

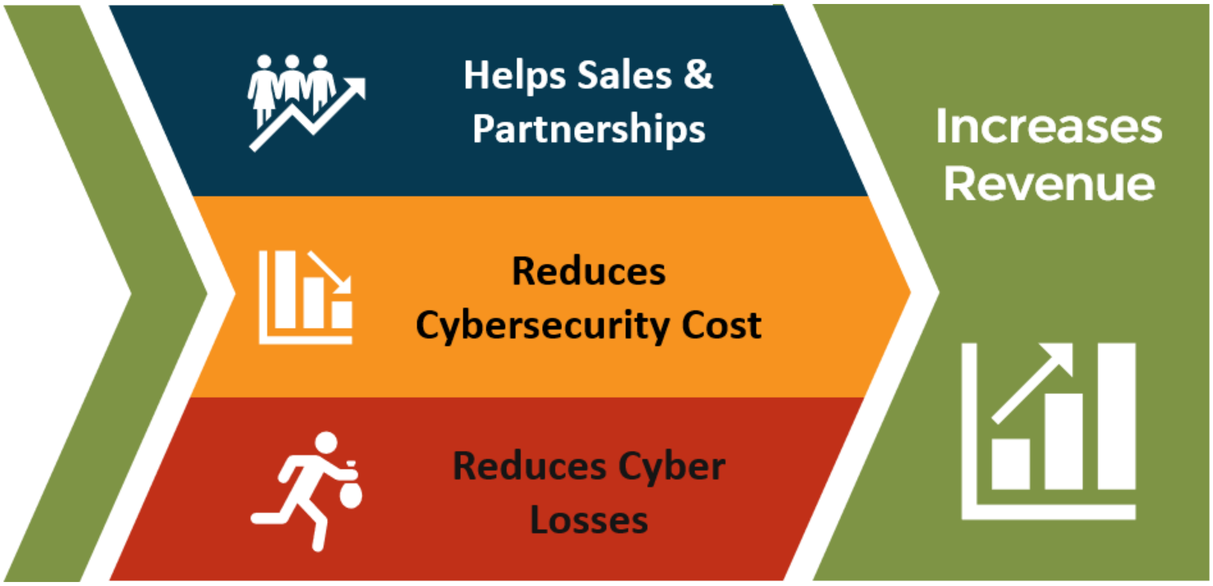


FIGURE 1: OVERVIEW OF REVENUE-CENTRIC CYBERSECURITY

Though not a comprehensive "how-to" guide, the rest of this document helps organizations learn how to leverage Revenue-Centric Cybersecurity.

DEPLOY THE 4-PART CYBER RISK MITIGATION CYCLE

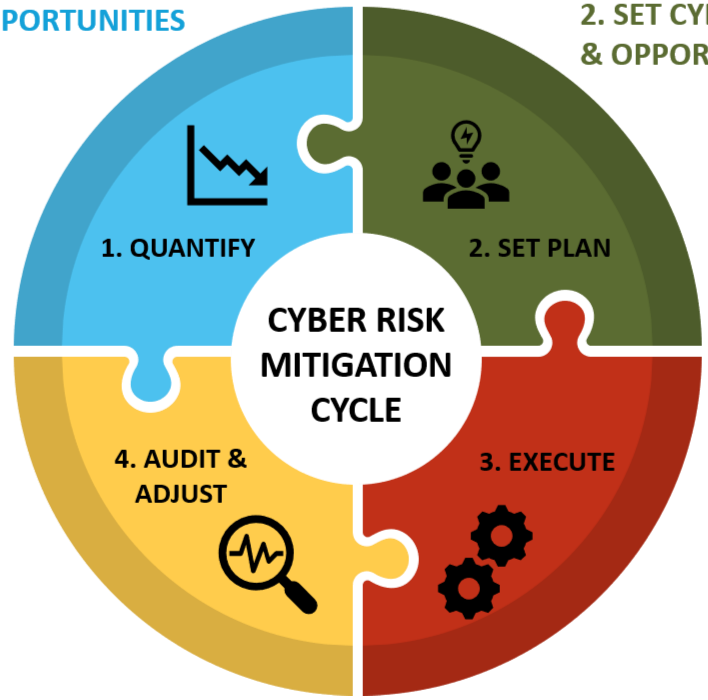
The key to leveraging Revenue-Centric Cybersecurity is to properly and continuously deploy the 4-Part Cyber Risk Mitigation Cycle introduced by Figure 2 (below). This Cycle efficiently organizes how to cost-effectively mitigate your unique cyber risks and develop the cybersecurity proof to best drive revenue. Before reading the rest of this document, which summarizes the Cycle's four parts, we recommend studying Figure 2. It will help you understand each part of the cycle and how they fit together.

1. QUANTIFY RISKS & OPPORTUNITIES

- Set & deploy a Multidisciplinary Team.
- Assess & quantify your Unique Cyber Risks & Opportunities.

2. SET CYBER RISK MITIGATION & OPPORTUNITY PLAN

- Create a 2-Part Cyber Risk Mitigation System with Auditing & Adjustment.
- Allocate Resources among the 5 Mitigation Tools.



4. AUDIT & ADJUST

- Effectively implement your auditing system.
- Adjust your Cyber Risk Mitigation & Opportunity Plan as needed.

3. EXECUTE THE PLAN

- Implement your Cyber Risk Mitigation & Opportunity Plan.
- Use customized Cyber Incident Mitigation Protocols, not a typical incident response plan.

FIGURE 2: THE 4-PART CYBER RISK MITIGATION CYCLE

TIPS FOR UNDERSTANDING THE 4-PART CYBER RISK MITIGATION CYCLE

1. Each part is connected to the others and has multiple steps.
2. Part 2's "Cyber Risk Mitigation & Opportunity Plan" should show how you will allocate resources among the 5 Mitigation Tools (see Appendix B) and specify how you will audit and adjust all your efforts.
3. Part 3 "Execute the Plan" focuses on implementing your plan.
4. Part 4 "Audit & Adjust" focuses on properly auditing and improving your plan.

SECTION 1. OVERVIEW OF THE CYCLE’S PART 1 “QUANTIFY RISKS & OPPORTUNITIES”

The Cycle’s Part 1 has two elements:

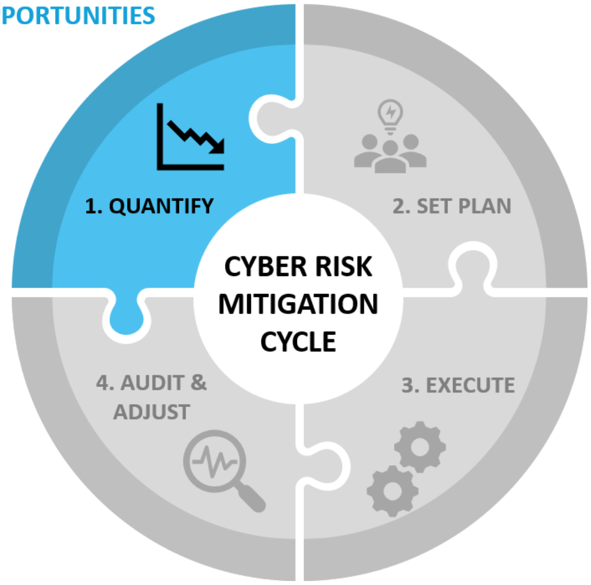
(A) Set & deploy your Multidisciplinary Team and

(B) Assess & quantify your Unique Cyber Risks and Opportunities.

The following summarizes each element.

1. QUANTIFY RISKS & OPPORTUNITIES

- Set & deploy a Multidisciplinary Team.
- Assess & quantify your Unique Cyber Risks & Opportunities.



A. SET & DEPLOY YOUR MULTIDISCIPLINARY TEAM

The right Multidisciplinary Team helps organizations properly implement every aspect of Revenue-Centric Cybersecurity. Critical parts of creating the right team include assigning the strong leadership, ensuring the leadership has the proper authority and budget, and allowing leadership to create, develop and leverage a multidisciplinary mitigation team covering these areas:

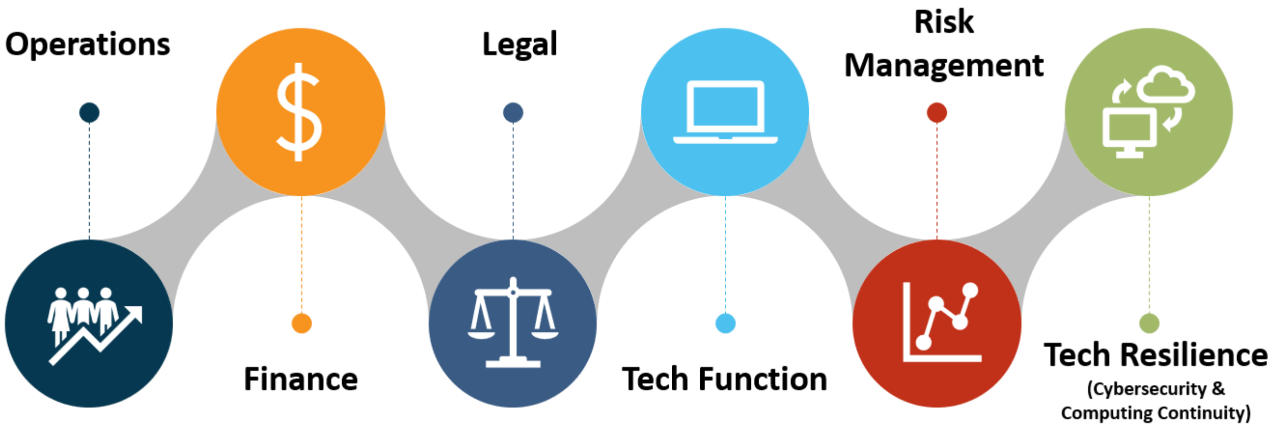


FIGURE 3: THE MULTIDISCPLINARY TEAM

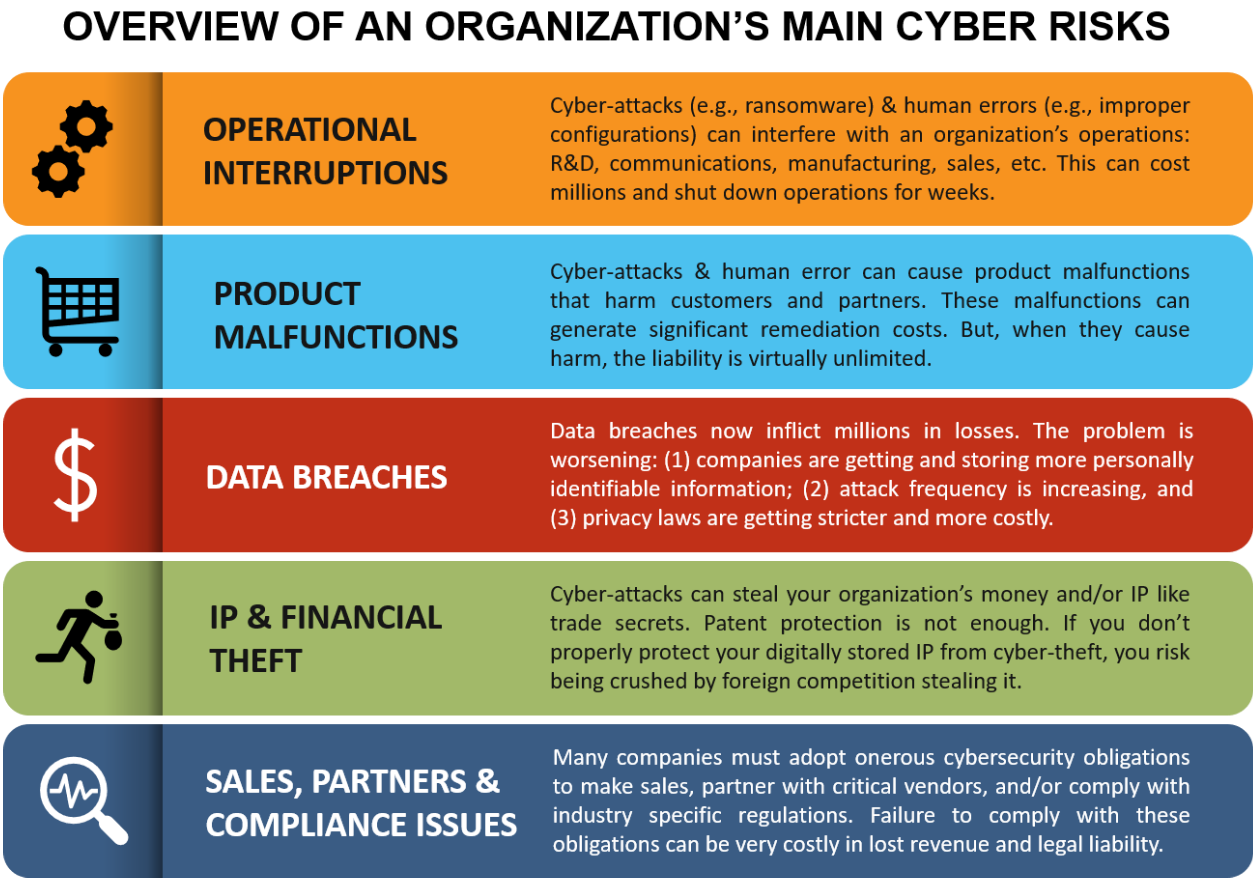
Some organizations already possess the internal multidisciplinary expertise needed to apply Revenue-Centric Cybersecurity; while others need to supplement with external help or training. The requisite talent, however, is not enough because (1) many organizations don’t how to use it, (2) many fail to implement the right leadership and/or goals, (3) existing corporate structures and traditional cybersecurity and risk-management practices get in the way, and (4) some internal resources need a “boost” to properly understand their role in multidisciplinary cyber mitigation.

Some common organizational traits, moreover, degrade the team’s effectiveness: e.g., (1) significant (and sometimes dangerous) deference to technologists as to operational cyber risks, (2) deficient oversight by finance and operations (particularly failure to quantify risks and properly prioritize, allocate, and audit limited mitigation resources), (3) ineffective and unnecessary separation between operational and product cyber risk mitigation, (4) a lack of multidisciplinary cooperation, and (5) failure to incorporate an intelligent cyber risk mitigation approach into product design. Therefore, when creating and implementing your team, remember to arm them with the right resources and knowledge.

B. ASSESS & QUANTIFY YOUR UNIQUE CYBER RISKS AND OPPORTUNITIES

Introduction to Cyber Risks: Your Cyber Risks comprise any threat that can interfere with your organization's profitable use of its digital data, software, and computing devices (i.e., any device using a CPU and/or IP address such as computers, mobile devices, printers, and IoT devices) collectively referred to as "Computing Technologies." This interference can be either operational (e.g., systems and info needed to deliver your offerings) and/or with your offerings (e.g., computing technology inside a pacemaker).

While every organization has a unique set of Cyber Risks, most Cyber Risks fall into these five categories:



OVERVIEW OF AN ORGANIZATION'S MAIN CYBER RISKS

OPERATIONAL INTERRUPTIONS

Cyber-attacks (e.g., ransomware) & human errors (e.g., improper configurations) can interfere with an organization's operations: R&D, communications, manufacturing, sales, etc. This can cost millions and shut down operations for weeks.

PRODUCT MALFUNCTIONS

Cyber-attacks & human error can cause product malfunctions that harm customers and partners. These malfunctions can generate significant remediation costs. But, when they cause harm, the liability is virtually unlimited.

DATA BREACHES

Data breaches now inflict millions in losses. The problem is worsening: (1) companies are getting and storing more personally identifiable information; (2) attack frequency is increasing, and (3) privacy laws are getting stricter and more costly.

IP & FINANCIAL THEFT

Cyber-attacks can steal your organization's money and/or IP like trade secrets. Patent protection is not enough. If you don't properly protect your digitally stored IP from cyber-theft, you risk being crushed by foreign competition stealing it.

SALES, PARTNERS & COMPLIANCE ISSUES

Many companies must adopt onerous cybersecurity obligations to make sales, partner with critical vendors, and/or comply with industry specific regulations. Failure to comply with these obligations can be very costly in lost revenue and legal liability.

FIGURE 4: AN ORGANIZATION'S MAIN CYBER RISKS

Introduction to Opportunities: Opportunities refers to any financial advantages that your organization can obtain by persuading clients, partners, and strategic buyers that it and its offerings are cybersecure. Each organization has a unique set of opportunities.

To more fully understand the concept of Opportunities, consider this example using a medical device manufacturer producing a new connected pacemaker. To begin selling a new connected pacemaker, the manufacturer must obtain FDA approval, which requires a clinical trial in collaboration with a healthcare deliver organization like a hospital. Because the hospital and the manufacturer will be jointly and severally liable for any patient harm the pacemaker inflicts – e.g., physical injury or data breach – they have shared Cyber Risks. An obvious shared Cyber Risk is any cyber-attack that causes the pacemaker to malfunction and thereby harm patients.

In this context, before the hospital will agree to the trial, it should require that the manufacturer "prove" its device is sufficiently cybersecure. This typically comes in the form of an agreement the manufacturer must sign that details the cybersecurity that it must have adopted. After a manufacturer's successful clinical trial with the first hospital and FDA approval, the manufacturer will still need to prove its cybersecurity to every additional hospital to which it wants to sell its devices. Therefore, when setting its customized Cyber Risk Mitigation and Cybersecurity Opportunity Plan, the manufacturer should identify what it needs to do to create the "proof" of its cybersecurity to drive revenue.

Overview of Quantifying Cyber Risks

Quantifying Cyber Risks with a high degree of accuracy can be complex, time-consuming, and not necessarily worth the effort. But, understanding what is at stake is essential, helping you properly allocate and optimize your limited budget. To help you quantify your unique cyber risks, we have defined three broad but helpful categories of Cyber Risk Quantification:

Intense: If your organization has the resources and motivation to obtain a higher degree of accuracy, consider reading the book How To Measure Anything In Cybersecurity Risk by Douglas W. Hubbard and Richard Seiersen. The book addresses in-depth the challenges of cyber risk quantification and provides a series of insights and suggestions that can be used for what the authors claim to be a more accurate quantification methodology.[ii] We have found that most organizations need not use this Intense approach.

Moderate: A moderately accurate approach is to apply the FAIR Model for Risk Measurement. FAIR stands for factor analysis of information risk. It is an open international risk model developed to improve the effectiveness of risk measurement. For a helpful publicly available guide to applying the FAIR Model, read the Open Fair Risk Analysis Process Guide. The Open Group also provides interactive Risk Analysis tools and FAIR training and certifications to help organizations master and apply the FAIR model.

Basic: This involves roughly estimating the likely financial harm from your unique cyber risks and current cyber risk mitigation efforts, particularly your cybersecurity. When just starting to adopt Revenue-Centric Cybersecurity, this is often the best approach because many companies have not yet diligently and cost-effectively applied the 5 Mitigation Tools summarized in Appendix B. In many situations, this "Basic" level of quantification can help identify vulnerabilities that require immediate attention and are a much higher priority than the diminishing marginal utility of more accurate quantification.

Regardless of your quantification approach, we recommend that your organization apply these three basic steps:

Identify Your Unique Potential Loss Events: A Unique Potential Loss Event (UPLE) is a specific result from a cyber-attack or cyber malfunction that can inflict financial harm on your organization. To help identify your organization's UPLEs, consider starting by using the 5 Cyber Risk Categories summarized in Figure 4 on page four to identify your unique Cyber Risks; and then list the specific ways that the occurrence of your unique Cyber Risks – e.g., the theft of specific digital IP, a company-wide ransomware attack, a product malfunction injures clients, different types of data breaches – can harm your organization.

Estimate Financial Harm from each Unique Potential Loss Event: For each of your UPLEs, your multidisciplinary team should estimate the different amounts of financial harm that would be inflicted based on differing degrees and types of risk occurrence. For example, the financial harm from ransomware attacks often depend on the duration of their interference with your operations – which means that you should model the harm based in part on duration of interference.

Estimate Unique Potential Loss Event Frequency: This involves an integrated assessment of the (1) frequency of the underlying threat and (2) your organization's ability to prevent and/or mitigate the harm from the threat.

For more info, see Appendix A.

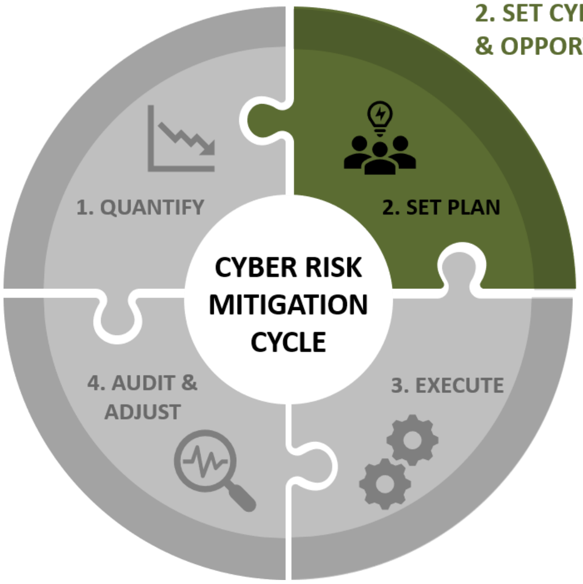
SECTION 2. OVERVIEW OF THE CYCLE'S PART 2 "SET REVENUE-CENTRIC CYBER RISK MITIGATION & OPPORTUNITY PLAN"

A Cyber Risk Mitigation and Opportunity Plan should be a dynamic document that explains how your organization will cost-effectively mitigate its Cyber Risks to an acceptable level and produce the cybersecurity proof needed to drive revenue.

While a detailed "how-to" is outside the scope of this document, it introduces the two most important aspects of these plans:

(A) Creating a Cyber Risk Mitigation System; and

(B) Using the 5 Cyber Risk Mitigation Tools.



2. SET CYBER RISK MITIGATION & OPPORTUNITY PLAN

- Create a 2-Part Cyber Risk Mitigation System with Auditing & Adjustment.
- Allocate Resources among the 5 Mitigation Tools.

A. CREATE A 2-PART CYBER RISK MITIGATION SYSTEM

Cyber Risk Mitigation Systems help you implement the 4-Part Revenue-Centric Cycle (explained above) by making it easier to organize your efforts. Figure 5 below and the following explanations help you understand how to create one of these systems:

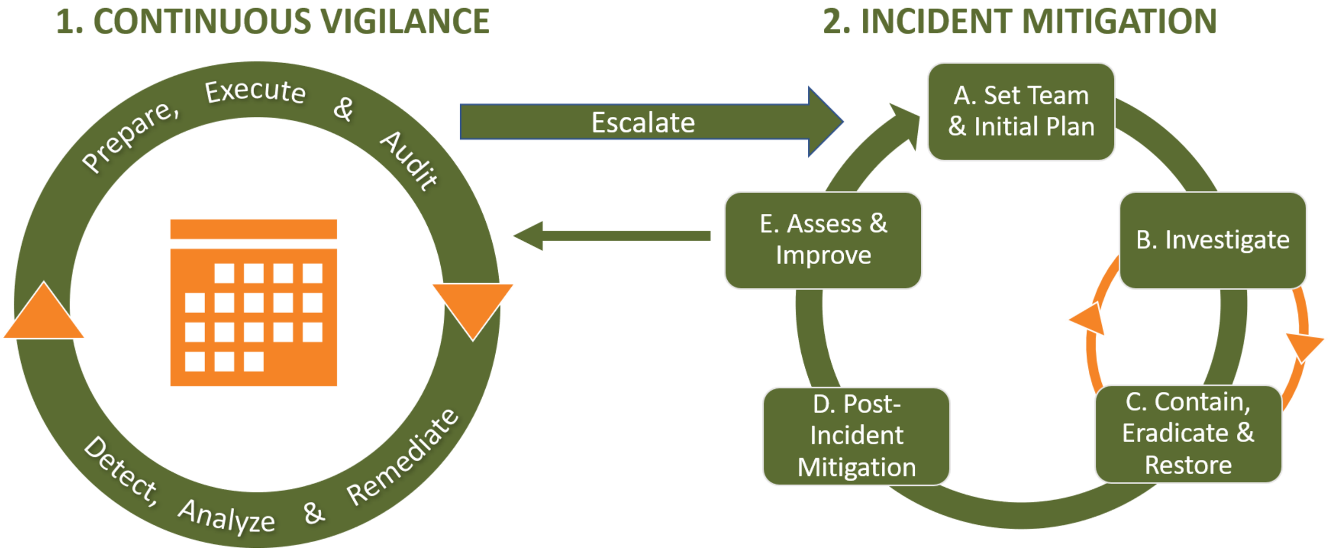

1. CONTINUOUS VIGILANCE
2. INCIDENT MITIGATION
Prepare, Execute & Audit
Detect, Analyze & Remediate
Escalate
A. Set Team & Initial Plan
B. Investigate
C. Contain, Eradicate & Restore
D. Post-Incident Mitigation
E. Assess & Improve

FIGURE 5: CYBER RISK MITIGATION SYSTEM OVERVIEW

Continuous Vigilance: It is everything organizations should do before an exigent cyber incident requires immediate mitigation:

> **Prepare:** This covers the Cycle's Part 1 (Quantify Risks & Opportunities) and Part 2 (Set a Cyber Risk Mitigation & Opportunity Plan), including creating your Incident Mitigation Protocols. Figure 2 on page 2 shows the Cycle.
>
> **Execute:** This includes the Cycle's Part 3 (Execute the Plan).
>
> **Audit:** This includes the Cycle's Part 4 (Audit & Adjust).
>
> **Detect & Analyze:** The systems, technologies, and people your organization will use to identify and analyze cyber vulnerabilities and incidents (e.g. cyber-attacks or malfunctions).
>
> **Escalate:** The process your organization will use to escalate material cyber incidents to your Incident Mitigation Protocols.

Incident Mitigation Protocols: These comprise the system your organization will use to reduce the harm from exigent cyber incidents:

> **A. Set Team and Initial Plan:** You will set a mitigation team for each specific, escalated cyber incident. The team will create an initial investigation, containment, eradication and restoration plan based on the detection and analysis evidence.

B. Investigate: This is the investigation portion your initial plan, which yields the information to contain, eradicate, and/or restore operations. Sometimes, you'll proceed directly to the contain, eradicate, and restore phase.

C. Contain, Eradicate, and Restore: Contain is stopping the damage. Eradicate is removing any malicious code and/or unauthorized access. Restore is returning to normal operations. The loop accounts for the possibility that an organization will have to conduct multiple investigations that can lead to multiple instances of containment, eradication and/or restoration.

D. Post-Incident Mitigation: Reduces post-incident harm via things like regulatory notifications, privacy notifications, litigation, and/or public relations efforts.

E. Assess and Improve: Improves your overall Cyber Risk Mitigation System by incorporating lessons learned.

These systems are a powerful tool for improving your ability to mitigate all your cyber risks.

B. ALLOCATE RESOURCES AMONG THE 5 MITIGATION TOOLS

Traditional cybersecurity – i.e., the technologies, people, and processes used to prevent and mitigate cyber-attacks – is just one of the five tools that your organization should consider for mitigating its Unique Cyber Risks. The following infographic (Figure 6) introduces the 5 Tools and the fact that you should have an auditing and adjustment system covering all your mitigation efforts.

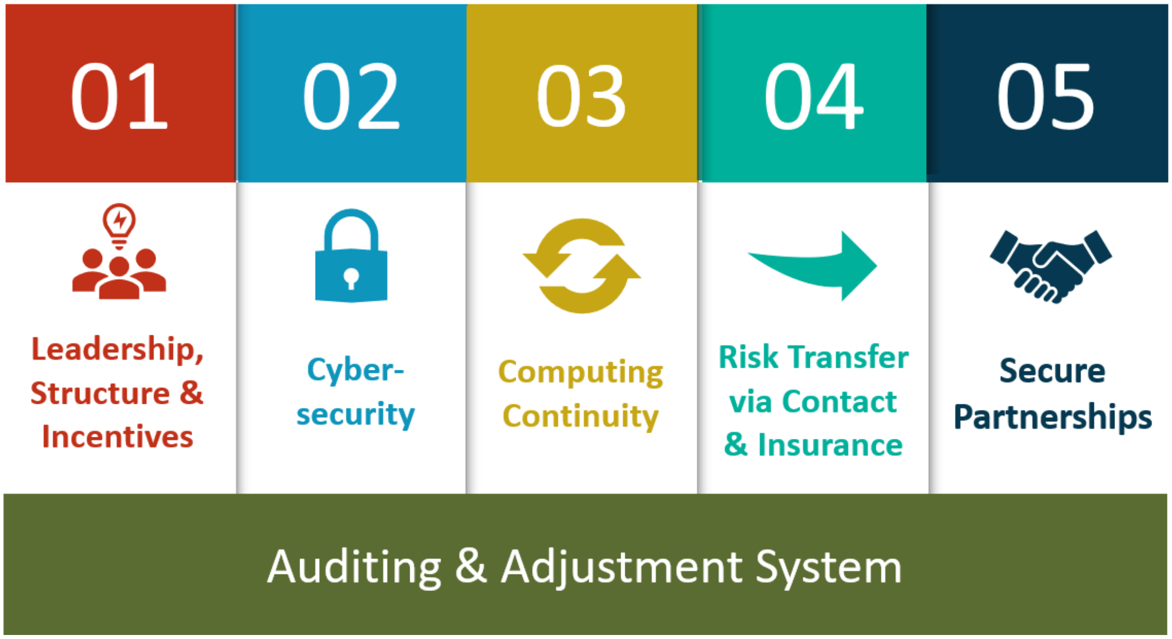
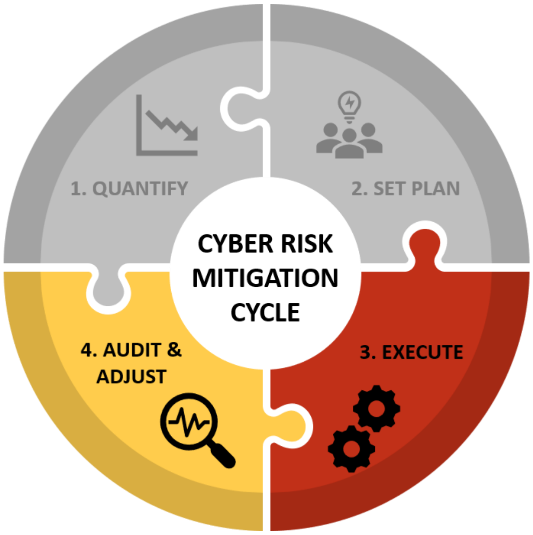

01
Leadership, Structure & Incentives
02
Cyber-security
03
Computing Continuity
04
Risk Transfer via Contact & Insurance
05
Secure Partnerships
Auditing & Adjustment System

FIGURE 6: THE 5 MITIGATION TOOLS

Revenue-Centric Cybersecurity helps you efficiently allocate your limited mitigation resources among the 5 Cyber Risk Mitigation Tools so you can cost-effectively reduce your organization's exposure to financial losses from cyber risks to an acceptable level. Appendix B explains these 5 tools in more detail.

SECTION 3. OVERVIEW OF THE CYCLE'S PART 3 "EXECUTE PLAN" & PART 4 "AUDIT & ADJUST

This section gives an integrated overview of the Cyber Risk Mitigation Cycle's Part 3 "Execute and Part 4 "Audit & Adjust."



4. AUDIT & ADJUST

- Effectively implement your auditing system.
- Adjust your Cyber Risk Mitigation & Opportunity Plan as needed.

3. EXECUTE THE PLAN

- Implement your Cyber Risk Mitigation & Opportunity Plan.
- Use customized Cyber Incident Mitigation Protocols, not a typical incident response plan.

A Critical Part of Execution and Auditing – a Detailed Implementation Plan

A critical part of creating your 2-Part Cyber Risk Mitigation System is preparing a detailed Implementation Plan that explains everything your organization has committed to do to mitigate its cyber risks. The plan comprises a set of checklists that detail each part of your Cyber Risk Mitigation System – including (1) exactly what needs to be done, (2) who is responsible for doing it, and (3) how you will audit (i.e., ensure it is done). When creating your Implementation Plan, consider how you can "automate" the execution and auditing of each part of your Cyber Risk Mitigation System. Many of the technologies you will deploy – e.g., a firewall or intrusion detection system – can be configured to automatically show an audit trail of what they've done. Other parts such as auditing how you are using contracts to shift shared cyber risks cannot be easily automated.

More about Auditing

There's a growing trend to hire an outside third-party to audit your cybersecurity, which is one of the remediation efforts that Equifax made in response to its devastating 2017 data breach. A good outside auditor will provide multiple benefits: (1) act as an additional "check" on the efficacy of your overall Cyber Risk Mitigation System; (2) ensure that you've properly implemented your Cyber Risk Mitigation System; and (3) help you identify cost-effective adjustments. The main problem with outside auditing is rising costs. To reduce auditing costs, look for ways to automate both execution and auditing, as the next section illustrates.

What the Equifax Data Breach Teaches About Auditing

To learn about why auditing your cyber risk mitigation efforts is so important, consider reading Appendix C. It summarizes the devastating 2017 Equifax Data Breach and how basic auditing might have prevented a billion-dollar loss.

THE NEXT THREE PAGES explain how Practical Cyber can help you leverage Revenue Centric Cybersecurity.

OVERVIEW OF HOW PRACTICAL CYBER CAN HELP

MULTIDISCIPLINARY EXPERTISE: Our core is a multidisciplinary integration of two experts (Dr. Rogers & Elliot Turrini) that we supplement with other experts as needed:

Cybersecurity Expert – Purdue University's Dr. Marc Rogers

Internationally known cybersecurity expert and founder of MKR Forensics.

Executive Director Purdue Cybersecurity Programs (one of the top programs in the nation).

25+ years practical cybersecurity experience enhanced by academic career.

Privacy & Cyber Lawyer + Cyber Risk Expert – Elliot Turrini

Former federal cybercrime prosecutor, cyberlaw/privacy attorney in private practice, & tech company General Counsel.

Cyber risk mitigation expert, including use of contract & insurance to transfer risk.

Co-Editor & Author of Cybercrimes: A Multidisciplinary Analysis.

ENTREPRENEURIAL APPROACH: Our CEO, Elliot Turrini, an experienced entrepreneur, helps ensure that you don't over-spend on cyber risk mitigation and on the cybersecurity proof you need to drive revenue. He used his entrepreneurial and business experience to lead the creation of Revenue-Centric Cybersecurity, an important innovation in cybersecurity, and our relevant services described in the next section.

CUSTOMIZED ASSISTANCE: Each organization has a unique starting point, risks, needs, talent, and resources. After we assess your situational needs, we draw from a set of powerful options to efficiently help you make progress toward Revenue-Centric Cybersecurity. We customize our assistance to your current and future needs.

OVERVIEW OF OUR RELEVANT SERVICES

OPTION 1 – C-SUITE SANITY CHECK

Deliverables: A one-hour initial consultation with Professor Marc Rogers and Elliot Turrini.

Benefits: Valuable, immediate advice that helps (1) mitigate your most glaring cyber risks and (2) set a smart, cost-effective ongoing strategy.

Costs: $1,975 for the hour consultation. It costs an additional $2,500 for a written summary of our initial advice.

OPTION 2 – CUSTOMIZED REVENUE-CENTRIC CYBERSECURITY ROADMAP

Deliverables: After analyzing your unique business model, we provide a high-level, prioritized, and customized Revenue-Centric Cybersecurity Roadmap. It is a set of customzied recommendations for how to better mitigate your unique cyber risks and best prepare cybersecurity proof for your opportunties.

Benefits: Helps you cost-effectively reduce your cyber risks via immediate changes, provides a roadmap for using Revenue-Centric Cybersecurity, helps materially reduce all your future cybersecurity costs, and paves the way for increasing revenue..

Costs: The costs range from as little as $10K and up to $75K. The main variables of cost are (1) the organization's size, (2) the complexity of its unique cyber risks, (3) its current mitigation efforts, and (4) the amount of effort that the organization wants from Practical Cyber.

OPTION 3 – ENHANCED EXTERNAL CISO SERVICES

Deliverables: Acting as an integrated mix of Chief Information Security Officer, Privacy/Cyber Lawyer, and Cyber Risk Manager, Dr. Rogers and Elliot Turrini can deliver any customized mix of these services. This includes what is often called virtual CISO services plus a lot more. Learn more here.

Benefits: Helps you costly effectively mitigate your unique cyber risks. Helps set your organization on a course for efficient growth and profitability. We provide security endorsements that can help persuade prospects, customers, investors, buyers, and/or partners about your security.

Costs: We offer two options –

(1) Fixed price annual agreements: They specify exactly what we'll do. The cost depends on the extent of assistance we provide. But, the costs will be up to 70% less than the approximate $236,000 per year it costs for a talented, full-time CISO. And, we provide more than CISO services, extending to privacy/cyber lawyer and cyber risk management.

(2) Time and materials: Companies can use this Brain Trust as needed on a time and materials basis for a blended rate of $350 per hour. Volume discounts available for prepaid bundles: 25-50 hours at $325 per hour; 51-100 at $300 per hour; and 101+ at $275 per hour.

THE VALUE WE DELIVER

- ❖ **BETTER MITIGATE POTENTIALLY DEVASTATING CYBER-ATTACKS**
- ❖ **SIGNIFICANTLY REDUCE MITIGATION COSTS**
- ❖ **FACILIATE SALES, COLLABORATIONS & PROFITABLE EXITS**
- ❖ **GIVE YOU PEACE OF MIND AND HELP YOU GROW**

MORE INFORMATION: For more information contact Elliot Turrini at (201) 572-4957 or Elliot@PracticalCyber.com.

APPENDIX A: QUANTIFICATION

Regardless of your quantification approach, it is important to understand that it is impossible to predict precisely the amount of financial harm that cyber-attacks will inflict in any given year – for these reasons (among others):

- Even assuming there was publicly available accurate historical records of the amount of financial harm inflicted by prior cyber-attacks – which there are not – your organization would need to apply those insights to its current situation without knowing both (1) how your mitigation efforts compared to those of the prior victims and (2) the future probability of cyber-attacks; and
- Historical cyber-attack data are not necessarily predictive of future cyber-attack prevalence and harm intensity.

We, therefore, recommend that you apply a quantification approach that focuses on estimating all the financial harm from a set of fairly common cyber-attacks – e.g., including ransomware, data breach, theft of IT stored digitally, interference with your offerings. To do this, we recommend organizing your efforts around the 5 main categories of Cyber Risk set forth in Figure 4 on page 4 and assuming a worst-case scenario in each category.

Here’s an example using a ransomware attack. Assume that most if not all your computers have been infected with a ransomware attack that has encrypted the data on the hard drives. In this situation, your main remediation options include:

(1) Try to decrypt the data;

(2) Pay the ransom and hope the attackers will (a) give you the information needed to decrypt and (b) not have installed programs inside your network that will allow them to launch another ransomware attack or inflict other harm; and

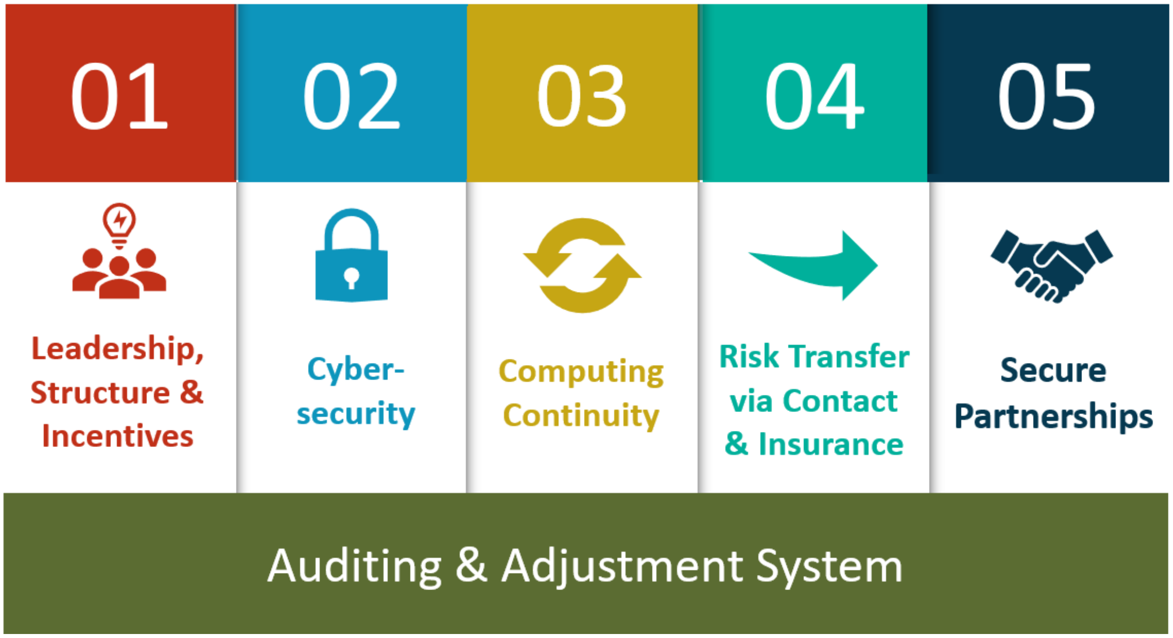
(3) Recreate your entire computing operations by installing a set of clean operating system, applications/software, and data on your computers.[iii]

The financial harm inflicted will depend on many factors, including (for example) (1) the remediation option you selected, (2) that option’s efficacy, cost and restoration speed, and (3) the negative impacts of lost productivity and/or product delivery while your computers are not working. A helpful exercise for setting the right ransomware remediation plan is do the following:

- Assume your organization will suffer a major attack;
- Roughly estimate the financial harm from lost productivity and/or product delivery via temporal increments – e.g. hours, days, weeks – that are the most relevant to your organization;
- Roughly estimate the costs of improving your “Computer Continuity” – i.e., your ability to restore full computing function – and of implementing it quickly enough to keep your financial losses within acceptable levels.

This information will help you decide which is the best option in this scenario. One caveat is to consider the uncertainty of future attack from the same cyber-attackers when paying the ransom.

APPENDIX B: SUMMARY OF THE FIVE CYBER RISK MITIGATION TOOLS


01
02
03
04
05
Leadership, Structure & Incentives
Cyber-security
Computing Continuity
Risk Transfer via Contact & Insurance
Secure Partnerships
Auditing & Adjustment System

LEADERSHIP, STRUCTURE & INCENTIVES: The right leadership, organizational structure and incentives are critical to effective cyber risk mitigation but difficult to implement. They make all the other techniques more effective. A detailed discussion of how to use this tool is outside the scope of this document. Contact us for more information.

CYBERSECURITY: It comprises all your efforts to prevent and limit unauthorized access, use, and/or interference with your computing devices (i.e., any device using a CPU and/or IP address such as computers, mobile devices, connected devices like printers, and IoT devices), software, and digital data – collectively referred to as "Computing Technologies." These efforts typically include:

(1) Technologies (e.g. firewalls, anti-virus, EDRs, SIEMs, data encryption);

(2) People (e.g. info security professionals, cyber lawyer, risk managers);

(3) Policies and processes (e.g. cyber incident response plan, training, compliance, security policies); and

(4) Training (e.g., employee cybersecurity training, professional development for your cyber risk mitigation personnel, cyber-attack simulation training).

COMPUTING CONTINUITY: Computing Continuity refers to the technologies, people, and processes that restore your Computing Technologies to their original operational state after a harmful cyber incident. Cyber incidents can include cyber-attacks or any other event (e.g. fire) that interferes with your Computing Technology operations. Because it is almost inevitable that cyber-attacks will in some way interfere with your Computing Technology operations – particularly because of rapidly growing ransomware threat – Computing Continuity is a critical aspect of cyber risk mitigation.

RISK TRANSFER VIA CONTRACT: Organizations often share cyber risks with their customers, vendors, and partners: e.g. (1) joint and several liability for injuries to customers caused by a defective offering, (2) the often-overlooked shared security responsibility model used by cloud computing vendors, and (3) dependence on a partner's computing infrastructure for your operations. The right contractual provisions can help mitigate "shared cyber risks"; while the wrong ones can shift millions to your balance sheet. While your lawyers likely have the general contracting expertise that is part of what's needed, some will benefit from our expertise with the cyber risk aspects.

RISK TRANSFER VIA INSURANCE: Using insurance to transfer cyber risks can be effective but terribly complex. You will need to consider how different policies – e.g. cyber liability policy, errors and omissions, and product liability – converge to mitigate your cyber risks. This is called a gap analysis, which requires accurately:

(1) Understanding each relevant policy;

(2) Identifying your actual, unique cyber risks;

(3) Quantifying those risks; and

(4) Estimating the efficacy of your other cyber mitigation efforts.

Some in-house lawyers and risk managers lack the time and/or expertise to conduct a proper "gap analysis" for cyber risks. Practical Cyber can materially improve their ability to use insurance to mitigate your cyber risks.

SECURE PARTNERSHIPS: With "shared cyber risks" contractual risk transfer is sometimes not enough. A cybersecurity chain is only as strong as its weakest link. Therefore, an organization's best cyber risk mitigation efforts can be undone by a partner's deficient cybersecurity. Would you prefer no problems because you "helped" partners become secure, or suing them to recover your losses from their cyber-insecurities? This highlights the need for your multidisciplinary team to help critical "partners" properly secure their portion of the shared cyber risks. We call this mitigation technique Secure Partnerships.

AUDITING & ADJUSTMENT SYSTEM: A critical part of Revenue-Centric Cybersecurity is preparing a detailed Implementation Plan that explains everything your organization has committed to do to mitigate its cyber risks. The plan comprises checklists that detail each part of your Cyber Risk Mitigation System (See Figure 5 page 6) – including (1) exactly what needs to be done, (2) who is responsible for doing it, and (3) how you will audit (i.e., ensure it is done). This comprises your auditing system. Additionally, your multidisciplinary team will be responsible for constantly looking for ways to make adjustments that improve efficacy and/or reduce costs.

APPENDIX C: THE EQUIFAX STORY

The Equifax Breach illustrates the importance of proper execution and auditing: In the spring of 2017, hackers gained access to Equifax's internal network by exploiting a known vulnerability in the Apache Struts Web Framework software running the server that Equifax used for its online dispute portal. Exploiting this vulnerability gave the hackers system-level control over the portal. The hackers then used existing encrypted communication channels to connect to the portal and send queries and commands to other systems inside the Equifax network. This allowed them to find and steal the personally identifiable information (PII) of about 145 million people stored inside Equifax's network. Their use of encryption blended their PII theft into Equifax's regular network activity, thusly allowing them to avoid detection by Equifax's scanning software.

According to the United States Government Accountability Office's August 2018 "Data Protection" Report about the Equifax breach, two auditing failures were the main causes for this devasting breach:

1. **Communication failure relating to vulnerability patching:** After receiving a US CERT vulnerability notice in March 2017, Equifax circulated the notice among their systems administrators. But, because the recipient list was old, the individuals responsible for installing the necessary patch didn't receive it. In addition, although the company scanned the network a week after the Apache Struts vulnerability was identified, the scan did not detect the vulnerability on the online dispute portal.

2. **Failure to properly implement network traffic analysis tool:** An expired digital certificate contributed to the attackers' ability to communicate with compromised servers and steal data without detection. Specifically, while Equifax had installed a tool to inspect network traffic for evidence of malicious activity, the expired certificate prevented that tool from performing its intended function of detecting malicious traffic.

Had Equifax properly implemented an auditing system for its patch management and security tool configurations, it would likely have not suffered this devastating data breach that inflicted over a billion dollars in losses.

APPENDIX D: SUMMARY OF WAYS WE HELP

Practical Cyber can help your organization in many ways. Drawing from the following options, we customize how we help your organization mitigate its cyber risks.

CYBERSECURITY & PRIVACY IMPROVEMENTS: We can help improve all aspects of your cybersecurity & privacy protections – (1) technologies (e.g. firewalls, anti-virus, EDRs, SIEMs, data encryption); (2) people (e.g. info security professionals, cyber lawyer, risk managers); (3) policies and processes (e.g. cyber incident response plan, training, compliance, security policies); and (4) training (e.g., employee cybersecurity training, professional development for your cyber risk mitigation personnel, cyber-attack simulation training).

COMPUTING CONTINUITY EFFICACY: Computing Continuity refers to your ability to fully restore all computing operations after a cyber-attack. Cyber-attacks that interfere with your business operations are almost inevitable – particularly because of the rapidly growing ransomware threats. This makes computing continuity critical. Because we have found that some organizations have not properly set up and/or tested their Computing Continuity, we include this option in our services.

CYBERSECURITY ENDORSEMENTS: There are times when an organization needs a cybersecurity expert to provide an endorsement about the strength of its cybersecurity. This need can arise with customers, partners, vendors, and/or strategic buyers. We provide effective, objectively valid cybersecurity endorsements.

PREPARATION OF INCIDENT MITIGATION PROTOCOLS: A critical part of cyber risk mitigation is effectively responding to cyber incidents, which can literally save you thousands if not millions. To do so, you need to prepare and practice a set of customized Incident Mitigation Protocols, which are more effective than traditional incident response plans. For more information consult Figure 5 on page 6 and the related information.

PROFESSIONAL DEVELOPMENT FOR STAFF: We can help your cybersecurity staff develop professionally. We provide customized development plans for each person. Because Dr. Rogers has been a preeminent cybersecurity professor, his mentoring delivers substantial value.

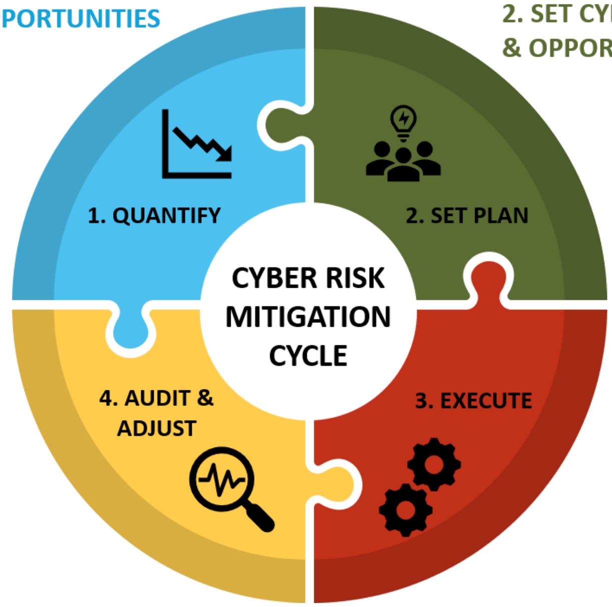
IMPROVE YOUR CONTRACTUAL MITIGATION: Companies often share cyber risk with their customers, vendors, and partners. The right contractual provisions are critical for transferring shared cyber risks. While your lawyers have the general contracting expertise that is part of what's need to succeed in this area, some will benefit from our cyber risk expertise. We, therefore, can help you use contract to mitigate your cyber risks.

IMPROVE YOUR INSURANCE MITIGATION: Using insurance to mitigate cyber risks can be effective but terribly complex. But, some organizations lack the time and expertise needed to conduct a proper "gap analysis" for cyber risks, and simply rely on an insurance broker. That can lead to material problems and high-costs. With Practical Cyber's help, your legal and risk-management resources can materially improve your ability to use insurance to better mitigation cyber risks.

TUTORING OF INDIVIDUAL TEAM MEMBERS: Because not every member of your team has the required knowledge and expertise, we offer additional tutoring of team members to help bring them up to speed. This can help you more quickly become self-sufficient.

ORGANIZATIONAL ADJUSTMENTS: Even small adjustments to your leadership, structure and incentives can materially improve the efficacy of your cyber risk mitigation.

SET & EXECUTE A DETAILED ANNUAL SCHEDULE ORGANIZED BY THE CYBER RISK MITIGATION CYCLE: We can help you create a detailed annual schedule organized around this Cyber Risk Mitigation Cycle:



1. QUANTIFY RISKS & OPPORTUNITIES

- Set & deploy a Multidisciplinary Team.
- Assess & quantify your Unique Cyber Risks & Opportunities.

2. SET CYBER RISK MITIGATION & OPPORTUNITY PLAN

- Create a 2-Part Cyber Risk Mitigation System with Auditing & Adjustment.
- Allocate Resources among the 5 Mitigation Tools.

3. EXECUTE THE PLAN

- Implement your Cyber Risk Mitigation & Opportunity Plan.
- Use customized Cyber Incident Mitigation Protocols, not a typical incident response plan.

4. AUDIT & ADJUST

- Effectively implement your auditing system.
- Adjust your Cyber Risk Mitigation & Opportunity Plan as needed.

Efficiently executing this schedule is critical to success. And, it helps your organization establish and maintain the type of candid, consistent and rapid communication needed for an effective Cyber Risk Mitigation System.

ASSESSMENT OF AUDITING EFFICACY: Auditing is a critical (often improperly implemented) aspect of cyber risk mitigation. One common reason is that many organizations have trouble analyzing the efficacy of their own operations because it is difficult enough to execute the strategy without having to audit it. We, therefore, can help you assess the efficacy of your auditing system for cyber risk mitigation in ways that (1) identify and rectify deficiencies and (2) prevent your organization from suffering preventable losses due to cyber-attack. For an illustration of the power of auditing, consider reading the Equifax story in Appendix C.

ASSISTANCE TO THE BOARD OF DIRECTORS: In some instances, companies will benefit from Practical Cyber talking with their boards. This assistance can help the board (1) appreciate the benefits of cyber risk mitigation and (2) more proactively and effectively execute its cyber risk mitigation oversight responsibility.

[i] The traditional cybersecurity approach is typified by NIST's Cybersecurity Framework's five functions: identify, Protect, Detect, Respond and Recover. While the NIST Cybersecurity Framework offers very helpful high-level information about how to use cybersecurity (e.g., technologies, people, and processes) to prevent cyber-attacks and mitigate the harm they inflict, it is not a revenue-centric system. Because it was not written by people responsible for driving revenue, it fails to fully embrace today's economic realities – particularly the need to quantify Cyber Risks and Cybersecurity Opportunities; and how to properly leverage all 5 Mitigation Tools as

detailed in Appendix B. Moreover, Revenue-Centric Cybersecurity incorporates, improves, and builds upon the best aspects of the NIST Cybersecurity Framework, which helps make it a natural advancement in the evolution of cybersecurity. Another limitation is how the NIST Framework does not help organizations implement the right Leadership, Organizational Structure and Incentives. While the Framework talks about "Governance", it does not provide anywhere near the details that organizations need to properly use the mitigation tool of "Leadership, Structure & Incentives".

[ii] A detailed summary of the book's recommendations is outside the scope of this document.

[iii] We recommend a complete recreation when you cannot with a high degree of certainty know that the attackers have not installed other malicious code on your computing devices that will allow them to commit future crimes if you only remedy the affective computing devices.