Introduction to *An Example Cybersecurity Plan*

Hello. If you're reading this, it's likely in conjunction with the LIMSwiki-hosted *Comprehensive Guide to Developing and Implementing a Cybersecurity Plan*. This example cybersecurity plan was built as a necessary consequence of developing that guide, which addresses what goes into meeting cybersecurity goals based on industry standards and cybersecurity frameworks. The cybersecurity plan is one of the most important components of that process.

You're also likely reading this because you intend to develop (or modify) your own cybersecurity plan. It's important to remember that your cybersecurity plan should be a living and breathing document. As new information is discovered, related policies are updated, and new IT components added, those changes may very well affect portions of the cybersecurity plan. All too often businesses find themselves creating policies and plans, only to have them collect dust, never getting updated with changing times. One or more people should have the explicit assignment of reviewing and updating the cybersecurity plan at regular intervals.

Also know that this example plan goes one step further with the "living document" analogy, perhaps in what some will consider an unorthodox fashion. As referenced in Section 9, on communication, this example plan is presented from the standpoint of a fictional company that early on agreed "to an iterative release approach" for its cybersecurity plan, "rather than waiting for all development to be complete before sharing the plan." This means that in its fictional universe, ABC123 Co. chose to create a 1.0 version of its plan—mostly as a scaffolding—and released it to its staff, despite the plan still being far from complete. With each significant update (i.e., a 1.x release), staff get to see a storyline develop, experience the document incrementally come to life while also, as a result, witness the research results of its "IT and Cybersecurity Modernization Team" filter in and fluidly shape the growth in other sections of the plan as it develops. The fictional company justifies this approach through the lens of transparency and the opportunity to "increase overall buy-in of the plan itself."

You'll notice a Version 1.6 on the plan, and that the language clearly states that while nearing completion several components of the plan are being still being researched. Presenting an example cybersecurity plan in this way also benefits you, the reader, in that it you get a glimpse into the development process of the plan, from the standpoint of the fictional company. This doesn't mean your cybersecurity plan need be approached in the same way. However, the 10 suggested development steps from Chapter 5 of my *Comprehensive Guide to Developing and Implementing a Cybersecurity Plan* should somehow still be addressed with your plan. And remember—demonstrated clearly in this example plan—that referencing external but related policies and documents is encouraged to keep the plan more concise and effective.

For reference, the 10 steps, and their sub-steps, are:

1. Develop strategic cybersecurity goals and define success
    a. Broadly articulate business goals and how information technology relates
    b. Articulate why cybersecurity is vital to achieving those goals
    c. State the cybersecurity mission and define how to achieve it, based on the above
    d. Gain and promote active and visible support from executive management in achieving the cybersecurity mission

2. Define scope and responsibilities
    a. Define the scope and applicability through key requirements and boundaries
    b. Define the roles, responsibilities, and chain of command of those enacting and updating the cybersecurity plan
    c. Ensure that roles and responsibility for security (the “who” of it) are clear
3. Identify cybersecurity requirements and objectives
    a. Detail the existing system and classify its critical and non-critical cyber assets
    b. Define the contained data and classify its criticality
    c. Identify current and previous cybersecurity policy and tools, as well as their effectiveness
    d. Identify the regulations, standards, and best practices affecting your assets and data
    e. Identify and analyze logical and physical system entry points and configurations
    f. Perform a gap analysis
    g. Perform a risk analysis and prioritize risk based on threat, vulnerability, likelihood, and impact
    h. Declare and describe objectives based on the outcomes of the above assessments
    i. Identify policies for creation or modification concerning passwords, physical security, etc., particularly where gaps have been identified from the prior assessments and objectives
    j. Select and refine security controls for identification, protection, detection, response, and recovery based on the assessments, objectives, and policies above
4. Establish performance indicators and associated time frames
    a. Determine baselines and indicators based on the assessments and objectives from the previous step
    b. Determine how to measure progress and assess performance (quantitative vs. qualitative) and what tools are needed for such measurement and assessment
5. Identify key stakeholders
    a. Determine what internal entities or people may act as cybersecurity stakeholders
    b. Determine what external (federal, state, local, and private) entities the business currently interacts with
    c. Define how those stakeholders shape the cybersecurity plan and its strategic goals
6. Determine resource needs
    a. Determine whether sufficient in-house subject-matter expertise exists, and if not, how it will be acquired
    b. Estimate time commitments and resource allocation towards training exercises, professional assistance, infrastructure, asset management, and recovery and continuity
    c. Review the budget
7. Develop a communications plan
    a. Address the need for transparency in improving the cybersecurity culture
    b. Determine guidelines for everyday communication and mandatory reporting to meet cybersecurity goals
    c. Determine guidelines for handling or discussing sensitive information

    d. Address incident reporting and response, as well as corrective action
    e. Address cybersecurity training methodology, requirements, and status tracking
8. Develop a response and continuity plan
    a. Consider linking a cybersecurity incident response plan and communication tools with a business continuity plan and its communication tools
    b. Include a listing of organizational resources and their criticality, a set of formal recovery processes, security and dependency maps, a list of responsible personnel, a (previously mentioned) communication plan, and information sharing criteria
9. Establish how the overall cybersecurity plan will be implemented
    a. Detail the specific steps regarding how all the above will be implemented
    b. State the major implementation milestones
    c. Determine how best to communicate progress on the plan's implementation
10. Review progress
    a. Monitor and assess the effectiveness of security controls
    b. Review how to capture and incorporate corrective action procedures and results
    c. Determine how often to review and update the cybersecurity plan
    d. Determine external sources for "lessons learned" and how to incorporate them for improving cybersecurity strategy

Best wishes with your cybersecurity endeavors,

Shawn E. Douglas

Document version: 1.0

ABC123 Co. Cybersecurity Plan

IT and Cybersecurity Modernization Team

M.T. Anderson A.R. Davenport

S.A Smith B.A. Turnbull

Version 1.6, March 2020
Doc. ID ABC123-CyPlan1.6-03-20

Summary

In light of events that nearly compromised the integrity of its proprietary and partner data, ABC123 Co., an environmental laboratory services company, has decided to formally develop and adopt a cybersecurity strategy and enforce it across its operations. We believe that cyber threats will only worsen in severity and number and recognize the growing importance of taking protective measures more seriously for the future longevity of the company. We also believe that by implementing and enforcing a well-documented and meaningful cybersecurity plan based on existing standards, ABC123 Co. will be better prepared to meet or exceed the requirements of a changing regulatory atmosphere, by extension. A key component of ABC123 Co.'s cybersecurity strategy is a cybersecurity plan that takes into account industry-standard guidance such as the National Institute of Standards and Technology (NIST) Special Publication 800-53 and the NIST Cybersecurity Framework.

This document is the product of activities undertaken since August 2019, with some of those activities still ongoing. This is a living document, meaning that it continues to be updated as we make new discoveries, identify more vulnerabilities and threats, and make changes to other related support and policy documents in the organization. Despite its continuing evolution, it still attempts to provide a clear picture of our cybersecurity plan, describing the methods, technology, training, and enforcement activities to be adopted by ABC123 Co. It also describes activities still pending, which will further shape the plan itself going forward. Finally it also makes reference to additional related company documents, e.g., the *ABC123 Co. Business Continuity and Security Plan*, to make this cybersecurity plan more concise (rather than rehashing large chunks of text from those documents).

Acronyms and Abbreviations

APHL	Association of Public Health Laboratories
BI	business intelligence
COTS	commercial off-the-shelf
CRM	customer relationship management
EDD	electronic data deliverable
ERLN	Environmental Response Laboratory Network
IT	information technology
LIMS	laboratory information management system
NIST	National Institute of Standards and Technology
P&P	process and procedure
SaaS	software as a service

Contents

Introduction

ABC123 Co. is an environmental laboratory services company dedicated to making "the most accurate analyses, on-time and within budget." The company has been in business since 2007 and operates three laboratory facilities, as well as a small, separate headquarters for administrative personnel. These facilities had for a period of time largely depended on manual processes to operate, with computers being used primarily for administrative and laboratory results tracking purposes. In 2015, owner Maria Anderson saw a need for more automated methods within ABC123 Co.'s operations, particularly with the then-potential addition of a third laboratory. Prior, laboratorians had been using Microsoft Excel sheets to track analytical results, but the practice rapidly became antiquated.

In 2016, an open-source laboratory information management system (LIMS) solution was trialed to better manage the increasing flow of results data, but ultimately it didn't meet our laboratories' needs. Users found the solution lacking in several areas, and we didn't have the in-house programming expertise to modify the source code. Additionally—and more importantly—we discovered in late 2018 that test methods proprietary to ABC123 Co. were nearly compromised, as was confidential client information, including demographics, billing information, and analytical results. Fortunately, we determined, the resulting damage was minimal. Yet had the configuration of our open-source informatics solution not been updated just days prior, we fear the digital attacker would have done more long-term damage. In the end, we found the security features of the trialed LIMS solution lacking, and without any dedicated LIMS support services, a new software solution was required.

In August 2019, we began discussing more robust long-term informatics solutions with commercial developers of LIMS. Ms. Anderson foresees untapped potential in environmental testing services, as well as possible cross-over into agricultural testing services, including cannabis testing. Given the regulatory expectations placed on laboratories in that industry, past events here at ABC123 Co., and the anticipated investment in a new LIMS solution (with business intelligence [BI] components such as billing and operational analytics), it was time to also address the cybersecurity needs of our growing company.

We have since identified the technological, staffing, and training needs that will come with the addition of a new LIMS, upgrades to our existing infrastructure, addition of business intelligence, and potential moves into even more regulated markets. This was done through a rigorous process of identifying key stakeholders in these activities and organizing the company IT and Cybersecurity Modernization Team to develop a robust cybersecurity strategy that still fits within our goals and budgeting while also addressing how ABC123 Co. protects not only its own interests but also the interests of current and future stakeholders, including clientele.

This cybersecurity plan is a central portion of the company's overall cybersecurity strategy. It describes our overall approach to cybersecurity, including strategic goals, scope, responsibility, requirements, performance indicators, identified stakeholders, resource requirements, communications strategy, business continuity, implementation, and review requirements, consistent with other new and revised documentation within the company.

1. Cybersecurity Goals and Envisioned Successes

Business goals

ABC123 Co., at its core, strives for "the most accurate analyses, on-time and within budget." We are providing an essential service as an environmental testing laboratory, ensuring water sources are potable, watersheds are safer, and air quality is monitored appropriately. Additionally, with the potential to move into agricultural testing this decade, we may also find ourselves responsible for ensuring the safety of products derived from plants such as cannabis. As such, people depend on us to provide accurate test results every time, on-time, and at a price point that is acceptable along the demand curve.

As our workflow and process improvement have become more technological since our humble beginnings, we have added tools such as Microsoft Excel, customer relationship management (CRM) software, an open-source LIMS, and an online results portal. The way we work and the data resulting from that work have changed since we started in 2007. The adoption of these and other tools has, however, always been as a means to better meeting our goals of **accurate, timely testing while keeping overhead costs low**.

Why cybersecurity?

Today we find ourselves moving to a new LIMS after trialing a free open-source option. In late 2018, we were forced to deal with the aftermath of an attempted cyberattack that originated from our front-end web-hosted results portal. Thankfully the damage was minimal, but it opened management's eyes that even a small business such as ABC123 Co. might be targeted for cybercrime. We have since learned that cyber attacks on small businesses like ours are actually not unusual, and cybercrime rates continue to rise at alarming rates around the world. Additionally, nearly 60 percent of small and midsize businesses go bankrupt within six months because of the fallout from a cybersecurity incident. If ABC123 Co. continues to integrate more web-exposed technologies and continues to expand physical operations, a cybersecurity strategy that addresses both the digital and physical protection of company and client data is increasingly vital to ABC123 Co.'s longevity.

Cybersecurity strategy

ABC123 Co. will strive to **reorganize**, **integrate**, **maintain**, periodically **evaluate**, and responsibly **encourage** the use of its information technology (IT) and software systems in such a way so as to ensure the long-term security of its digital (and physical) assets that contribute to its overall success within the laboratory industry. (We call this strategy **RIMEE**, for short.) As such, we must:

- reorganize our existing hardware and software solutions, removing those solutions that are deemed insecure, unsustainable, and otherwise detrimental to our success while thoughtfully adding solutions that can improve our success;

- integrate those solutions in such a way that we can reduce points of failure, improve operational workflow, and more readily stand to gain from using those solutions;
- maintain those solutions in such a way that we limit points of cyber and physical intrusion to an agreed-upon risk level within the constraints of our staffing, budget, and goals;
- evaluate the effectiveness of those solutions and the policies surrounding them at periodic intervals to ensure our company and cybersecurity goals are still being met; and
- encourage the responsible use of those solutions in such a way as to minimize the risks associated with their use.

At every step of the way, it remains vital that we consider current and future stakeholders of this cybersecurity strategy, along with ABC123 Co.'s overall goals. We have both internal and external customers that require the integrity of business data and analytical results to remain intact. This includes a full process of analyzing our technological and operational needs; securely meeting those needs; responsibly operating, maintaining, and protecting the solutions involved; rapidly investigating and responding to all cybersecurity issues that may occur; and transparently overseeing their resolution. This will require buy-in from all levels of operation, as well as a clear and focused approach that involves training, practice, and periodic review.

Executive statement on this strategy

We love our business and what we do. We strongly believe in our goals as well, and as we integrate more technological solutions into improving how we accomplish those goals, it will require focus and dedication to cybersecurity to stay profitable and relevant in the laboratory industry. This requires a plan, like any other operation, and this cybersecurity plan is the result.

But management can't be the only group that believes in the value of this plan. We need everyone, from human resources to the laboratorians, to be onboard with the value of cybersecurity to meet our goals of accurate, timely, and affordable testing. Businesses fail all the time—and increasingly so—because the security of their digital and physical assets isn't taken seriously. We'd rather not be like those who fail but instead a shining example of success, in part because we didn't take for granted the security of our data.

Our small lab business, with its humble origins, has truly grown into something bigger. This change has brought with it wonderful things for staff, but also a few growing pains in the process. Change is always difficult to manage, but we intend to do our best with it to ensure the longevity of our business. We hope you continue to be along for the ride and help ABC123 Co. become the best it can be through training on and dedication towards keeping our operations safe and secure.

Best,

Maria Anderson
Owner and Manager, ABC123 Co.

2. Scope and Responsibilities

Scope

The stated **RIMEE** cybersecurity strategy will drive the scope of how we succeed with that strategy and meet both our business goals and cybersecurity objectives.

ABC123 Co.'s effort to reorganize, integrate, and maintain its existing hardware and software solutions requires not only research into the available commercial off-the-shelf (COTS) options, but also a clear understanding of the functionality needed from its systems. A significant determiner has been whether or not we have the in-house expertise and a strong desire to keep our systems in-house, and what applications, if any, will become third-party hosted software as a service (SaaS) solutions. How we define the logical and physical boundaries of our information management systems in part drives our cybersecurity effort, which itself requires a team of experienced and knowledgeable individuals—the "IT and Cybersecurity Modernization Team"—able to tie together our workflow needs, what COTS options exist, how they fit into our budget, and how much control we require.

We fortunately already have relatively clear process and procedure (P&P) and workflow documentation. (See both the General Policy folder and the department-level folders located on the F: drive.) However, as it seems increasingly likely that ABC123 Co. will attempt an expansion into the agricultural—and by extension, cannabis analysis—industry, the IT and Cybersecurity Modernization Team must also look at the laboratory workflows and regulatory concerns associated with that industry. If, for example, we go with a SaaS option and conduct cannabis analysis, can we host client information on a cloud server located in another country, like Canada? If we have the suitable budget, we may want to consider solutions that allow us to more readily expand in the future without compromising cybersecurity. Additionally, we shall consider what future security risks are most likely with any given expansion, and not simply what attack threats we expect today.

To recap, the narrowing of our scope depends on the following:

- Is ABC123 Co. comfortable with expanding the logical and physical boundaries of some of our systems to a third-party, externally hosting provider?
- Does ABC123 Co. plan on expanding to agricultural and cannabis testing in the next few years?
- Does ABC123 Co. have a clear understanding of what its operational and workflow needs are?
- What does the technology, training, and maintenance budget of ABC123 Co. look like for meeting our cybersecurity strategy?
- What are the most likely current and future risks to ABC123 Co. data and systems?
- Finally, what COTS options are available that mesh with the answers to above? If none, what are we willing to compromise?

As of version 1.6 of this plan, many of these scope questions have been answered, yet some of them have not. Regarding the first point, we largely feel comfortable with the option of expanding to a cloud-based COTS LIMS, and as such we've been expanding our understanding of the security measures implemented by cloud providers. However, the final decision on our LIMS vendor and service model is yet to be determined. As to the second point, we have decided to treat our cybersecurity planning as if

we are going to expand into more regulated agricultural testing, with the implicit understanding that it's not a guarantee. As such, we address point three by expressing that we've looked at the workflow needs of an agricultural sample testing laboratory and widen our cybersecurity plan's scope to include it, again even if we eventually don't move into that area.

Regarding the budget, we fully address it in Section 6 of this plan. The current and future risks are addressed in Section 3. The final point about COTS options will be answered once we select our LIMS solution. Given we're switching LIMS to better address security concerns, we expect features of the LIMS to align with our plan. Where they don't we'll adjust accordingly.

Responsibilities

Our senior laboratory technician, Gillian Scott, and information technology administrator, Darryl Malone, are serving as co-leads for developing, enacting, and updating this cybersecurity plan. Our administrative office manager, Carla Stroman, is lending her writing and training expertise to the cause as well and is the administrative lead. These three individuals are the key members of the IT and Cybersecurity Modernization Team, and they may recruit additional support help from our staff (or from an external consultant) when appropriate.

Project Co-lead and Laboratory Lead: Gillian Scott - Responsible for research, communication, and evaluation within our three laboratories. If you are performing analytical work in the laboratory, you'll take your cybersecurity questions and concerns to Gillian.

Other roles: physical laboratory security, primary laboratory tech support, documentation review

Project Co-lead and Technology Lead: Darryl Malone - Responsible for system research, implementation, maintenance, and evaluation across all our operations. However, Darryl will largely be interacting with Gillian and Carla to ensure information is passed down in a clear, relatively jargon-free manner.

Other roles: technological risk management and enforcement, secondary laboratory tech support, secondary administrative tech support, documentation review

Document Lead and Administrative Lead: Carla Stroman - Responsible for document maintenance, communication, and training across all our operations. If you are performing administrative, custodial, or sub-contracted work, you'll take your cybersecurity questions and concerns to Carla.

Other roles: physical administrative security, primary administrative tech support, documentation review, training development and scheduling, annual review lead

3. Cybersecurity Requirements and Objectives

Existing system

The successful application of **RIMEE** requires that we know where we are now, as well as where we're going. This means knowing what we already have in place, via information gathering. The IT and Cybersecurity Modernization Team has collected the following information:

- documentation of the physical location of all current cyber equipment, at a granular level, both written and photographic, to detail mountings and connections;
- available diagrams and other documentation detailing mountings and connections;
- documentation of physical and cabling connections between pieces of cyber equipment, including physical ports;
- documentation of make, model and serial number of cyber equipment, as well as current firmware version, if applicable;
- documentation of all current software in use, as well as versions;
- documentation of all network-capable laboratory instruments and firmware; and
- documentation of all network-related port information and configurations on not only scientific instruments but also routers and switches.

The resulting information was clearly organized in an asset management spreadsheet for future reference and updates. Whenever possible, asset type, risk level, and criticality level were assigned to each piece of hardware and software. The spreadsheet also notes whether each component communicates internally (within the physical confines of our buildings), externally (outside the physical confines of our buildings), both, or neither.

This information has contributed significantly to the revised gap analysis (described later), which is still in preparation.

Existing data

Around late 2014, our need for richer, more electronic data became overwhelmingly obvious. A 2010 report by the Association of Public Health Laboratories (APHL) on environmental laboratory data came to our attention at that time. While we weren't heavily leaning on the public side of environmental health, we anticipated the possibility of doing more with that, and, more broadly, recognized the insufficient nature of tracking results from analytical sequences in Excel. "A future goal is to move away from spreadsheets and towards machine-to-machine language," stated the APHL in its report.

As such, our existing data has become richer since then, but not without struggles. The open-source LIMS we've trialed since 2016 helped our data become richer, but we were still unable to tailor the system source code to better meet our rapidly growing needs. Additionally, our electronic data deliverables (EDDs) still are not as robust as we anticipated.

Today, that rich data is largely analytical data that in some cases is able to identify individuals. Additionally, with our short but significant foray into testing for private environmental research and development (R&D) businesses, the analytical results are of a proprietary and confidential nature. We, of course, have our own proprietary business data about test methods and financial numbers that must be protected too.

Borrowing from the University of Illinois, we have taken to classifying our data as "high-risk," "sensitive," "internal," and "public." With some effort, we estimate that roughly 10 percent of our data is high-risk, 70 percent of it is sensitive, 15 percent of it is internal, and five percent is public. A more rigorous review of our data may still prove useful, however.

Existing cybersecurity policy and tools

Cybersecurity policy at ABC123 Co. was generally lax until mid-2018. We began updating basic security controls within the open-source LIMS we tested, with the most robust component being password type and reuse controls. However, we had little in the way of role-based access in place, and policies on using portable storage devices were not particularly well enforced. Around November 2018, we actually began to draft new tentative policies, driven largely by our tech lead Darryl Malone. He identified some weaknesses we had in several of our systems approaches and began enacting a few of those changes right before the cyberattack that struck. Afterwards, Darryl fully updated policies, and we began enacting them in early 2019. (See the Information Technology > Cybersecurity > Policies folder chain on the F: drive.) We had Carla also begin implementing a few basic training sessions to introduce the new policies, but we've since paused them as we now attempt a complete overhaul of our systems and cybersecurity policy. We've also developed a "lessons learned" document since the cyberattack (also on the F: drive, Information Technology > Cybersecurity > Cybersecurity Incident Response), and the IT and Cybersecurity Modernization Team will be taking it into consideration, along with all our existing but scope-limited policy documents. Work has already begun on updating those existing documents, with some such as our business continuity plan already complete. We anticipate all those documents to be updated by April 2020.

Influencing regulations, standards, and best practices

Our Laboratory Director, Jean de Luc, has largely been responsible over the years for helping ABC123 Co. stay compliant and developing P&P guided by standards and best practices. He has pointed us to a free internet resource called LIMSpec, which has recently been updated to link a variety of laboratory-related regulations, standards, and guidance to an ASTM laboratory informatics standard, E1578-18. This has immediately given us further insight into what additional functionality we should consider to help ABC123 Co. not only be more compliant, but also be a more efficient and standardized laboratory. We were already more or less familiar with U.S. Environmental Protection Agency (EPA) Environmental Response Laboratory Network (ERLN) requirements, but we learned more from reviewing the LIMSpec document.

Jean has recommended we use LIMSpec in conjunction with National Institute of Standards and Technology (NIST) cybersecurity controls. In fact, we've also learned that the same group that created LIMSpec has also mapped its LIMSpec specifications to the controls of NIST Special Publication 800-53,

Revision 4. These documents and mappings have significantly helped with our cybersecurity planning and system implementation, while allowing us to move forward in a way sympathetic to the relevant regulations, standards, and best practices.

System entry points + gap analysis

Currently, our IT infrastructure, albeit small, is in-house, largely located in the administrative building. The current open-source LIMS is installed on a server, along with some Microsoft Office applications and a client-server CRM application. The labs are able to log in to the LIMS and other applications via a web browser, which requires an internet connection. Operation and administration files are also stored on the server in the administrative building (the F: drive), with extranet access supplied to the labs. We also have a web-based results portal for clients to view their results. Our corporate website is hosted with a service provider, separate from our infrastructure.

Physical access to the IT infrastructure at the admin building is protected by a mechanical keyless cipher lock that operates without power. Additionally, all people entering the building, including deliveries, are required to enter the admin building from the front double-door entrance. Keycard access into the main building exists, or the desk attendant can buzz guests in. We also have an emergency exit with a compliant locking free egress system. A swipe card system is used at the laboratories. Operational security is bolstered with pre-hire screenings, annual staff assessments, and controlled swipe card access during off-peak hours. (We follow some of the guidelines from the National Academy of Sciences.)

The laboratory informatics component of our IT infrastructure may change should we decide to go with a cloud-based COTS LIMS. However, we still anticipate, at least in the short term, hosting our office applications (Word, Excel, CRM) and the extranet, though we do recognize there are SaaS alternatives to these as well.

Policy-wise, we've had access control policies in place for physical, operational, and information access. (Again, see the F: drive, under General Policy.) However, some of those policies have not been upgraded since the 2018 cyberattack. The IT and Cybersecurity Modernization Team has taken to updating these and other policies throughout the system update, upgrade, and policy implementation process.

We performed a proper gap analysis in the wake of the late 2018 cyberattack. We identified issues with both how the online provider portal was configured and with email phishing schemes attempting to acquire log-in information. Additionally, our incident response was initially weak, as we didn't fully anticipate some of the issues we've had. We've since adopted a "not if, but when" approach, which underscores the development of this cybersecurity plan.

Darryl and his team are conducting a more stringent follow-up gap analysis on our current tech using NIST Special Publication 800-53, Revision 4. Gillian and Carla have been re-examining the National Academy guidelines, as well as a few other sources, to see what operational and physical updates need to be made. Darryl has noted there is a "Physical and environmental protection" section in NIST 800-53, which will also be incorporated into Gillian and Carla's efforts.

Risk analysis

An initial risk analysis (see the Information Technology > Cybersecurity folder chain on the F: drive) arrived in September 2018, not long before the cyberattack. We began making some configuration changes based on that analysis, which likely prevented more damage than we actually experienced from the cyberattack. A follow-up analysis is currently in process, progress pending completion of the gap analysis.

Our initial risk analysis identified the following as the most likely risks, based upon threat modeling and architecture analysis:

1. Unauthorized key card use - *Threat*: low; *Vulnerability*: low; *Likelihood*: low; *Impact*: low
2. Unauthorized portable media (e.g., USB drive) use - *Threat*: medium; *Vulnerability*: low; *Likelihood*: medium; *Impact*: medium
3. Email phishing for account credentials - *Threat*: medium; *Vulnerability*: medium; *Likelihood*: high; *Impact*: medium
4. Corporate website hijacking - *Threat*: medium; *Vulnerability*: medium; *Likelihood*: high; *Impact*: low
5. Unauthorized LIMS access - *Threat*: medium; *Vulnerability*: medium; *Likelihood*: low; *Impact*: high
6. Unauthorized provider portal access - *Threat*: high; *Vulnerability*: medium; *Likelihood*: high; *Impact*: high

Regarding the first item, while we recognize that human error can result in a misplaced or even stolen key card, the likelihood of anyone effectively and maliciously putting it to use is low. We already have policy encouraging lost or stolen key cards to be reported as soon as possible. Additionally, with electronic restrictions on key card use after-hours, someone would have to enter during business hours, bypass reception, and go unnoticed in the work space. Even if that were to happen, the individual would also have to have the credentials of someone to access a computer system.

Regarding portable media, it remains relatively easy to block any unauthorized USB media devices from being recognized on business computers using group policy settings. Very few of our scientific instruments use USB interfaces, and this as of yet has not caused issues. A white list of authorized serial numbers is used in those rare instances where a USB device needs to be used.

As for email phishing, we've had problems with this in the recent past and have attempted to raise awareness about the issue with policy, communication, and training. We're looking to add additional filtering tools to cut down on the reception of such emails as well.

Item four, corporate website hijacking, has turned into an issue due to our WordPress configuration. We never thought anyone would want to try to hack a laboratory website, but here we are. The solution has been relatively painless, however, with the addition of several security plug-ins and website configuration changes that prevent brute force and other types of attacks. We now receive alerts of malicious attempts to log in and haven't had any major issues. However, we also recognize that we need to add a scheduled, regular task to ensure the plug-ins remain updated.

Unauthorized LIMS access is still a concern, though we imagine moving from some of the flaws of the open-source solution we chose to a COTS solution that is focused on security will alleviate some of that concern. We still need to look at the LIMS options out there and compare them. We'll be revisiting this risk in the near future.

The final item, unauthorized provider portal access, hits home for us. It was one of the major problems we faced when identifying the points of access for the 2018 cyberattack. A *National Law Review* article raises the concept of multifactor authentication as an added layer of security for our provider portal (even though they reference a patient portal, and we don't deal with personal health information). Our current portal service does not, as of yet, offer this feature, and we're investigating what to do going forward.

Objectives

While we are still waiting for several of the research tasks mentioned in this section to be completed (e.g., COTS LIMS assessment, revised gap analysis), we believe a preliminary set of cybersecurity objectives based on what we know so far can be developed. These may be updated as we formalize completion of our revised gap analysis and risk analysis, as well as the decision on our replacement LIMS. However, we believe little will change for these preliminary objectives even after LIMS assessment and gap analysis are completed.

To reiterate, our cybersecurity goals are to **reorganize**, **integrate**, **maintain**, periodically **evaluate**, and responsibly **encourage** the use of the IT and software systems of ABC123 Co. in such a way "so as to ensure the long-term security of its digital (and physical) assets that contribute to its overall success within the laboratory industry." (**RIMEE**)

The following clearly states the objectives associated with the RIMEE cybersecurity strategy:

How do we **reorganize**? Our objectives there are:

- complete follow-up gap and risk analyses associated with our current hardware, software, and data management situations (*priority*: high; *measurement*: report results to leadership, integrate into cybersecurity plan);

- assess vulnerabilities associated with gap and risk assessment results and determine what investment of resources is required to correct or reduce the impact of the vulnerabilities (*priority*: high; *measurement*: report results to leadership); and

- remove hardware components and software unable to be updated or deemed to be too expensive to correct or update properly, replacing with something more secure without sacrificing vital functionality (*priority*: high; *measurement*: budget, vendor due diligence documentation, vendor demo).

How do we **integrate**? Our objectives there are:

- assess areas of functionality duplication and redundancy in software used within the business, as well as any potential, more unified replacement (*priority*: medium to high; *measurement*: budget, vendor due diligence documentation, vendor demo);

- assess areas of data management inefficiency (e.g., multiple storage locations, duplicate data entry, multiple data formats, inconsistent data), as well as any potential methods for reducing the inefficiencies (*priority:* medium to high; *measurement*: budget, report results to leadership); and

- assess areas of process and workflow inefficiency that could be automated to improve overall efficiency (*priority:* medium; *measurement*: budget, consult a system integrator, report results to leadership.

How do we **maintain**? Our objectives there are:

- refine the existing reactive and preventative maintenance methodology to be more agile, relying less on reactive efforts (*priority*: medium; *measurement*: review maintenance plan with leadership);

- develop a greater focus on network maintenance, including developing improved network documentation (*priority*: medium; *measurement*: review action plan and created documentation with leadership); and

- investigate the feasibility of including predictive maintenance into an overall maintenance strategy (*priority:* low; *measurement*: budget, report results to leadership).

How do we **evaluate**? Our objectives there are:

- schedule recurring cybersecurity risk assessments and take necessary action based on their findings, being sure to update any relevant documentation, including the overall cybersecurity plan (*priority*: high; *measurement*: report to stakeholders, review documentation);

- schedule recurring reviews of hardware, software, and network maintenance methods and schedules to ensure they are still relevant and timely (*priority*: medium; *measurement*: report to stakeholders, review documentation);

- schedule recurring security audits that include reviews of traffic logs, penetration tests, and other suitable methods, also ensuring that P&P and other related documentation is updated when changes are required based on the audit findings (*priority*: high; *measurement*: report results to stakeholders, review documentation); and

- schedule quarterly reports of cybersecurity metrics that are quantifiable, observable, and objective (*priority*: high; *measurement*: report results to stakeholders).

How do we **encourage**? Our objectives there are:

- ensure all levels of leadership are onboard and clear about the importance of cybersecurity to the longevity of the business (*priority*: high; *measurement*: discussions, meetings);

- improve subject-matter expertise among leadership by at least partially funding continuing education units (CEUs) (*priority*: medium; *measurement*: CEUs gained, demonstration of acquired knowledge);

- issue password and other access policies that strike a balance of being secure enough to meet business goals without being overburdening to staff (*priority*: low to medium; *measurement*: in-house surveys);

- take appropriate and fair corrective action when a misstep of cybersecurity policy occurs (*priority*: high; *measurement*: recognition of misstep, recognition of steps towards correction, annual cybersecurity plan review);

- support and encourage annual or biannual cybersecurity training exercises throughout the business, while documenting attendance (*priority*: high; *measurement*: test results); and

- maintain cybersecurity training and policy documents and clearly communicate to all stakeholders consequential changes when they occur (*priority*: high; *measurement*: assign task and evaluate progress).

Policies

Policy creation and update is largely addressed prior. However, we're asking the laboratory, administrative, and IT departments to review and update existing policies to ensure they address cybersecurity, where applicable. This includes laboratory technician welcome guides, administrative handbooks, and IT password policies, among others. This review and update process has been assigned to each department.

Additionally, we've identified a few new documents for creation and dissemination:

- this cybersecurity plan (*responsibility*: IT and Cybersecurity Modernization Team)
- a cybersecurity training manual (*responsibility*: Carla Stroman and Tyler Boman)
- a third-party cybersecurity requirements agreement (*responsibility*: Carla Stroman)
- network mapping and maintenance documents (*responsibility*: Darryl Malone)
- a corrective action policy for cybersecurity missteps (*responsibility*: Carla Stroman)

Cybersecurity controls

We have chosen a slightly modified version of the controls found in NIST Special Publication 800-53, Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations*. The creators of LIMSpec have created a simplified version of the controls, using most of the "Low" baseline controls, as well as a handful of "Moderate" and "High" baseline controls. Many of those controls are mapped to their LIMSpec document.

The IT and Cybersecurity Modernization Team reviewed these controls early in the plan development stage, which in turn guided many of the decisions made for the creation of this cybersecurity plan. The team agrees that these cybersecurity controls are sufficient for a relatively small environmental laboratory operation like ours. These controls act as recommended safeguards or countermeasures to protecting the integrity and availability of the information system, as well as the privacy and retention of the system's information. Some controls such as "MA-6 (2) Timely maintenance: Predictive maintenance" may not get implemented due to being impractical or not aligning with our budgeted objectives.

An explanation of the initially chosen controls can be found on the F: drive under the Information Technology > Cybersecurity > Security Controls folder chain.

4. Performance Indicators

It took time to grasp how best to handle metrics (performance indicators) to measure the success of our cybersecurity plan. We've consulted several texts, including the Electric Power Research Institute's (EPRI) *Cyber Security Metrics for the Electric Sector: Volume 3*, MITRE Corporation's *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring*, and MITRE's Cyber Resiliency Metrics Catalog.

As a small laboratory company, we're not too keen on making a significant investment into developing and tracking performance indicators, but we do see their value, particularly on the quantitative side. Appendix B of MITRE's document provides listings of objective-driven metrics. The IT and Cybersecurity Modernization Team started there, looking at matching our cybersecurity objectives with representative activities and metrics in their document. MITRE divides these activities and metrics into eight "cyber resiliency" objectives:

1. Prevent/Avoid: "Preclude the successful execution of an attack or the realization of adverse conditions"
2. Prepare: "Maintain a set of realistic courses of action that address predicted or anticipated adversity"
3. Continue: "Maximize the duration and viability of essential mission or business functions during adversity"
4. Constrain: "Limit damage from adversity"
5. Reconstitute: "Restore as much mission or business functionality as possible subsequent to adversity"

6. Understand: “Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity”
7. Transform: “Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively”
8. Re-Architect: “Modify architectures to handle adversity and address environmental changes more effectively”

Our team saw significant overlap in some areas of the MITRE objectives with our overall strategy of **reorganize**, **integrate**, **maintain**, **evaluate**, and **encourage** (**RIMEE**). For example, our “reorganize” objectives tie directly into MITRE objective eight, “re-architect.” MITRE’s “transform” objective feeds into not only several of our objectives, but also many of the transformative aspects discussed in this cybersecurity plan overall. We’ve tapped into EPRI’s idea of creating “security metric worksheets,” which have helped us link the representative activities and metrics we chose to NIST Special Publication 800-53, Revision 4 controls, responsible personnel, frequency of use for the metric, and more.

We’ve chosen a select number of appropriate representative activities and metrics and built out metric worksheets. These files can be found on the F: drive under the Information Technology > Cybersecurity > Performance Indicators folder chain. An example of one of these worksheets follows:

Field	Data
Internal Metric ID	**Incident Response 2 (Mean Time to Fix or MTTF)**
Goal	Measure the effectiveness of an organization or business unity to recover from incidents
Supporting MITRE Representative Activities and NIST SP 800-53 Controls	MITRE Activity and Sub-objective: Reconstitute, RE-S2-A1: Execute recovery procedures in accordance with contingency or continuity of operations plans NIST SP 800-53 Rev. 4 Controls: • Incident handling (IR-4) • Incident monitoring (IR-5) • Incident response plan (IR-8)
MITRE Metric or Measurement	Time between initiation of recovery procedures and completion of documented milestones in the recovery, contingency, or continuity of operations plan (in hours) [MT-37]
Type	Effectiveness/Efficiency
Environment	Since dates of occurrence and dates of recovery can be tracked manually, MTTF can be measured in either information technology (IT) or operational technology (OT) environments
Formula	$\sum(Date\ of\ Recovery - Date\ of\ Occurrence)\ /\ Total\ Number\ of\ Incidents$
Target	MTTF values should trend lower over time.
Applicable Standards and Requirements	CJIS Security Policy Appendix G.7; NIST 800-53, Rev. 4, IR-4(1) and IR-5; NIST 800-53, Rev. 4, SI-2
Frequency	Collection Frequency: Quarterly Reporting Frequency: Quarterly
Responsible Parties	Information Owner: Darryl Malone, IT Information Collector: Callie Jones, IT Information Customer: Darryl Malone, IT

Data Source	Security incident and event management (SIEM) systems, host logs, antivirus software, trouble-ticketing system, manual sources
Reporting Format	Bar chart of Time (week, month, quarter) versus MTTF (hours per incident)

5. Key Stakeholders

Internally, company leadership unequivocally supports cybersecurity planning and action. This includes the following key stakeholders or "promoters":

- Maria Anderson, Owner and Manager
- Jean de Luc, Laboratory Director
- Darryl Malone, IT Manager
- Carla Stroman, Office Manager

In more abstract terms, every staff member of ABC123 Co. is a stakeholder. Key stakeholders aside, staff are essentially "defenders," who have a vested interest in the company's success but may not have as high a stake in influencing cybersecurity. Their influence primarily exists in doing small but important things, such as actively participating in cybersecurity training and applying cybersecurity policy to their daily activities.

Externally, ABC123 Co. also has key stakeholders. Our original investor, BT Capital's Tom Brighthoff, still has a stake in the success of ABC123 Co., which includes limiting legal liability from unsecure information systems. Additionally, we consider our existing clients stakeholders. The security of their test results and personal information is relevant to their success, not just ours.

Since we initiated our cybersecurity planning project, we've involved our key internal stakeholders, as well as Mr. Brighthoff and representatives of the two largest clients we have, Sara Anne Loman of Loman Environmental and Daniel Tieg of Tieg Services. Finally, we've also reached out to our IT vendor for additional input as it relates to their systems. Our internal key stakeholders have been primary to our cybersecurity efforts, as has Mr. Brighthoff. Our senior laboratory technician, Gillian Scott, has also provided valuable input in our efforts, for which we have been thankful. Loman, Tieg, and our IT vendor have been secondary as far as policy shaping has gone, though their input on our provider portal and existing hardware system longevity has been invaluable.

6. Resource Requirements and Allocation

Managing the IT needs of a small business, with three lab locations and an administrative office, hasn't required overwhelming investment in resources, but ABC123 Co. recognizes that knowledge and skills are critical to the success of any endeavor. We've been thankful for the long hours IT Manager Darryl Malone and his assistant Tyler Boman have put in, especially recently with the latest cybersecurity efforts. Their expertise has been invaluable. We, as a business, were not proactive enough with putting their knowledge and skills to best uses. Since 2018, we've shifted to a "not if, but when" approach to

cyber intrusions, and they have been an important catalyst in prompting our business-wide attempt at a cybersecurity plan.

As such, we believe we have sufficient in-house expertise to accomplish our plan. If we lack anywhere, it's with understanding cloud computing and SaaS installations. However, we anticipate between Darryl and support from the COTS vender we decide upon, should we explore a cloud LIMS solution, we'll be covered. Worse case we will look into a short-term consultant to assist us with our decisions. Laboratory Director Jean de Luc and senior lab technician Gillian Scott have extensive experience working with connected systems in the lab, so we feel comfortable in that area. Darryl and Tyler will lend their support to the administrative office.

We don't expect a major upfront investment in training. Darryl and Gillian have requested a few CEUs to upgrade their cybersecurity knowledge, and we have determined we have room in our overall cybersecurity budget to allow for that. We will have to, however, develop cybersecurity training material and present it in an appealing way to the rest of our staff. Office Manager Carla Stroman has agreed to help with this task, and we have authorized overtime hours for her and an assistant to help complete that task. We don't anticipate the level of cybersecurity training required from staff to be too taxing, though we do expect to have annual refresher training.

Our overall cybersecurity budget (F: drive, Finance > Cybersecurity) appears reasonable. We believe we can have a positive impact with a relatively small budget. Leaving the new LIMS acquisition aside (considered a separate expenditure), the proposed cybersecurity budget was at an additional 12.8 percent of company total IT spend, and the approved amount came to an additional 11.2 percent of total IT spend. We were able to trim a few items from the proposed and still feel comfortable in being able to meet our cybersecurity objectives.

7. Communications Plan

Stakeholders fully agree that transparency is important in not only managing the effects of a cybersecurity incident but also improving the overall longevity and business culture of ABC123 Co. Clear, timely, and effective communication plays a significant role in those efforts. Fortunately, this has been a component of ABC123 Co.'s overall business philosophy from day one. For example, we already have a number of communication templates hosted on the F: drive, each for specific report types and scenarios. And our monthly newsletter serves as an additional avenue for communicating policy changes and new training, for those who may occasionally miss an emailed notice.

While none of this had been documented in an actual communications policy before—taken for granted almost, as just part of the business culture—we realized during cybersecurity planning that we should finally create a formal communications policy. This realization actually came about after the late 2018 cyberattack, but in discussing the requirements of a quality cybersecurity policy, we finally took action. (For the complete communications plan, which includes cybersecurity elements, see the F: drive, General Policy > Communications folder chain.) Not only have we documented our old practices but also added new practices that address how ABC123 Co. should handle communication of:

- cybersecurity incidents internally,
- cybersecurity incidents externally,
- corrective actions for those who violate cybersecurity policy,
- changes to cybersecurity and related policy, and
- confidential and sensitive information.

We've also taken other, related steps. We've formally organized an incident response team that consists of owner Maria Anderson, as well as Darryl Malone, Carla Stroman, and representatives of our formal legal counsel at Stern & Sons. Policy has been developed (F: drive, General Policy > Business Continuity > Cybersecurity Incident Response folder chain; discussed further, next section) to address, step by step, how a cybersecurity incident should be handled. This policy document encourages taking the necessary time to fully understand the scope of impact and its cause before sending out communication. The document also encourages that such communication addresses the corrective actions that will be taken, while avoiding jargon and imprecise language (e.g., "may" and "might"). The incident response team also recognizes the value of training drills to practice incidence response; budgeting has remained for this item in our cybersecurity budget.

Other types of training are valuable as well. What is training if not the communication of concepts and ideas to others? Insufficiently trained personnel are often the weakest component of a security perimeter, and ABC123 Co. wants to ensure that cybersecurity training is properly performed, while not being overbearing. Training schedules will be made, by department, for the initial training, then follow-up training will scheduled, for now at an annual interval. Changes to cybersecurity processes and training material will be clearly communicated via email and the newsletter by our administrative department.

8. Incident Response and Business Continuity

Our initial steps towards building out cybersecurity incident response (discussed in the previous section) were done separately, from an IT perspective. However, we quickly learned we could benefit by combining the IT perspective of response with the operational perspective of business continuity planning. This merger of incident response with our original *Business Continuity and Security Plan*, however, needed to overcome a few minor obstacles, including use of different terminology between IT and operations. Additionally we recognized that cybersecurity frameworks like NIST SP 800-53, Rev. 4 also address several of the physical and environmental systems protections already referenced in our business continuity plan, including fire protections, water damage protections, and emergency power. We also realized that the prior work of classifying criticality of systems for the old business continuity plan would need to be updated with the introduction of the incident response plan. These and other overlaps ultimately led us to redevelop the business continuity plan in tandem with the cybersecurity incident response plan, while also unifying terminology, incident classifications, response thresholds, and technology lists.

The revised business continuity plan sits at the top of the policy structure (F: drive, General Policy > Business Continuity), with the related cybersecurity incident response plan one layer down from that. They both, however, reference each other and explain their similar yet divergent purposes. Also at the top Business Continuity level you'll find application dependency mappings, which are also mirrored in the Information Technology folder chain. While these aren't vital for the average staff member to

understand, they do provide some of the underlying logic for why response plans were developed the way they were.

Finally, if there is at any point confusion about the chain of responsibility for business continuity and cybersecurity incident response, we've added a simple PDF (Incident_CoC.pdf) in the top structure of Business Continuity, showing the chain and associated contact information. It should be printed out and displayed in each department for quick reference, and updated when response policy is changed.

9. Implementation of This Cybersecurity Plan

The IT and Cybersecurity Modernization Team remains responsible for the development, implementation, re-evaluation, and maintenance of this cybersecurity plan. We anticipate the development of this plan will be completed shortly, as we primarily lack only a decision on our COTS LIMS solution, a revised gap analysis, and a revised risk analysis as of version 1.6 of this plan, and a couple of other small tasks, all nearing completion.

A beta version of our milestone document for guiding implementation of this cybersecurity plan has been drafted and can be found on the F: drive under the Information Technology > Cybersecurity > Implementation folder chain. Once the final plan development tasks are complete, the milestone dates of the implementation document may be updated slightly, but we don't anticipate much else to change. The milestone document includes milestones for expected deliverables, project phase transitions, evaluation, and other external events driving implementation. As of version 1.6 of this plan, we expect to complete initial implementation of this plan by September 2020, including necessary training and documentation. Consult the beta milestone document for full details.

We expect the biggest implementation disruptor, on the operational side, to be the new LIMS solution. Four months ago we began the tweaking of data entry standards and data field requirements, as well as the cleaning up of existing data, to aid with a more rapid transition to the new LIMS later this year. Our initial conversations with LIMS vendors have led us to believe that operationally swapping from the existing open-source LIMS to the new LIMS can occur relatively quickly and without significant disruption.

Regarding the communication of our cybersecurity planning activities, the IT and Cybersecurity Modernization Team agreed early on to an iterative release approach for our cybersecurity plan (rather than waiting for all development to be complete before sharing the plan). While this may seem unusual to the average business attempting to become cybersecurity-prepared, leadership agreed that the iterative communication approach has several advantages. This includes compliance with our efforts to be transparent about cybersecurity planning, as well as staff having the opportunity to witness the "living document" strategy in action.

As such, with each significant update (i.e., a 1.x release), staff were notified of the updated document, along with a convenient list of major changes to the document from the previous version. While leadership realistically expected few operational and administrative staff to pay much attention to these iterations, a small but surprising number of staff continued to be engaged with the updates to the

cybersecurity plan. We believe this sort of communication has, as a result, helped further increase overall buy-in of the plan itself.

Finally, a communication campaign of our overall strategy and objectives has supplemented the iterative releases of this plan. We recognize out staff have busy work lives, so we've tried to be as non-intrusive as possible while still communicating the development process. For now we continue to stick with email and the newsletter as primary communication methods, with the occasional meeting thrown in for significant updates and changes. A similar approach will be used for the implementation process, with more proactive communication as training sessions begin. The maintenance stage will be more low-key, though occasional updates on performance indicators, new cyber threats, and follow-up training will still be made.

10. Monitoring and Assessing Plan Effectiveness

The performance indicators and security metric worksheets discussed in Section 4 are a vital part of monitoring and assessing the effectiveness of this cybersecurity plan's implementation. However, we recognize it's not sufficient to simply use those metrics and call it "mission accomplished."

Those indicators and metrics may become inadequate in a number of ways. They may no longer effectively measure what we intended them to measure. The trends we expected to identify may no longer be accurate. Insufficient types or amounts of data may be making it the measures to be meaningful.

Similarly, the systems, their settings, and the procedures involving them may be revealed to be insufficient. Detection settings may need to be tweaked to stop attacks that are unexpectedly getting through, to accommodate new attack styles, or to reduce the amount of false positives generated. Personnel's assessment procedures may need to be tweaked, or they may need additional training to better understand cybersecurity metrics.

As such, quarterly reporting of cybersecurity metric results will also require an additional section dedicated to discussing any perceived gaps in collecting, measuring, and interpreting data related to cybersecurity metrics. A checklist has been created to streamline this discussion (F: drive under the Information Technology > Cybersecurity > Effectiveness folder chain). This reporting and checklist completion task will largely be the responsibility of our IT experts.

The cybersecurity plan itself is also not static; it must be re-evaluated and updated at regular intervals, as well as at critical moments of change. The IT and Cybersecurity Modernization Team remains dedicated to that re-evaluation and update process. Currently we believe an annual review will be sufficient, given that ABC123 Co. is still a relatively small business. However, that review schedule may change to biannual should we find, via our monitoring activities, that risk is greater than we anticipated in the long term. The annual review will take into account relevant metrics and the input of our declared stakeholders (likely through a quick online and anonymous survey). The team will then consider survey responses in parallel with the monitoring data, along with their own experiences. Additionally, the consideration of emerging cyber threats since the last review, as well as any relevant external incidents that affected other companies, will be factored into the review.

Additionally, we recognize that unanticipated or necessary change happens rapidly, requiring a more immediate re-evaluation and response. This often happens in the wake of a cyberattack or similar incident. The IT and Cybersecurity Modernization Team may be asked to take *ad hoc* action to updating the cybersecurity plan outside of the annual review to address any gaps in the plan as a result of addressing the cause of the incident. Additionally, when the annual review arrives, the "lessons learned" from that incident will be reviewed a second time to ensure the necessary changes are actually in place and are effective.

Finally, corrective action is an important component of evaluating the effectiveness of a cybersecurity plan. Is the same type of mistake occurring despite corrective action? For example, are staff still placing sticky notes with passwords in their open work space despite being advised of the risks associated with such activity, and being asked not to do it again? Why is it still a problem, despite our plan's best efforts? Examining the corrective action, its successes, and its failures can lead to additional insight. As such, the team will be examining corrective action response to missteps regarding (or intentional breaking of) the components of this cybersecurity plan.

Closing statement

This cybersecurity plan has attempted to address all the activities surrounding cybersecurity planning for our small laboratory business. Where details were not explicitly stated, references to supporting documents providing more details were provided.

ABC123 Co.'s cybersecurity strategy is the **RIMEE** strategy, one of **reorganizing**, **integrating**, and **maintaining** our IT infrastructure, while periodically **evaluating** it and our surrounding cybersecurity policies, while **encouraging** the responsible adoption and use of those policies and systems. Each element of RIMEE has its own set of objectives (Section 3), which help ABC123 Co. achieve the RIMEE strategy. This plan also addresses other important elements of cybersecurity planning, including risk analysis, gap analysis, stakeholder identification, budget and resource allocation, implementation, enforcement, effectiveness measurement, communication, and training.

If at any point questions arise from reviewing this plan, links to external supporting documents appear broken, or apparent omissions appear to exist in the content, contact your Department head on the IT and Cybersecurity Modernization Team (Section 2, Responsibilities). They are asked to provide assistance with these sorts of issues. As always, if the nature of your inquiry is sensitive, you can also approach Owner and Manager Maria Anderson.