The Common Sense Approach to Cybersecurity

By Cheryl Carmel

CISSP, security officer for OnSolve. member of (ISC)²

ONSOLVE™

Table of Contents

Cybercrime has changed the world of business as we know it, and no organization or individual is free from its hazards. With threat types including malware, ransomware, phishing attacks, fake news, identity theft and so many others, these attacks can block access to websites, capture identities, skim money, steal intellectual property and even track day-to-day activities of your organization or yourself.

These attacks are unpredictable and sometimes almost undetectable. The fact that such incursions are often not noticed until malevolent activity is well underway makes the problem all the more daunting. If you haven't reviewed your established business continuity plan with an eye towards enhancing cybersecurity, you're already behind.

If this sounds frightening, it should. Cybercrime is something to be very afraid of, especially if you let that fear drive to you to take action. We're all at risk, but there are many concrete things you can do to reduce your organization's risk. The reason why hackers are so good at their game is that they are exquisitely adaptable; to beat them, you must be adaptable too. Cybersecurity is not a one-time set of controls you can put in place, but an ongoing, changing and diligent effort. The best way to deal with cybercrime is to prevent it, so let's get started.

Build your cybersecurity program

Creating a program starts with the basic building blocks of the program itself and the framework you base the program on. The Deming cycle, or PDCA model, is an iterative cycle that starts with *Plan*, moves to *Do*, ensures you *Check* results and cycles to *Act*, or *Adjust*. This management model is the basis for many cybersecurity programs regardless of the framework you end up following. It allows new ideas to be put into action and ensures that they accomplish your intended goals.

Following a plan this way builds out your policy and procedure documents in tandem:

- Plan – starts the process
- Do – sets the plans into action and operationalizes them
- Check – ensures the monitoring and assessment of the tasks to meet goals
- Act – includes corrective actions to make continual improvement

In essence, you want to *prepare* for issues before they happen and *practice* for when that time comes.

There are lots of programs already available for you to draw on that follow existing business standards and regulations. Following an existing standard is not only a great way to get started on the process of prevention, but can make your program development more efficient in terms of tools, time and talent.

A good plan requires coordination between teams including, but not limited, to information security, privacy, business continuity, risk management and regulatory compliance. Each of these areas, in turn, must understand the needs of other areas outside their realm, like sales, marketing and other parts of the company. All your teams must work together to provide the best possible defense to prevent bad things from happening.

Core functions

Executive sponsorship

To build any program, you need buy-in at the highest levels. The executive team and your board of directors all need to be in agreement with the cyber-program initiative. How do you get their attention?

The key to getting and keeping the attention of those at the highest levels is to provide the right information in a clear, concise, educational format that ties directly to the business objectives.

Before asking for funding for your program, it's important you show the risk to the organization of *not* providing the funding. What damage to reputation or brand will occur if the company's name is in the headlines due to a data breach? The old adage, "all publicity is good publicity," is no longer true in the era of hacking, malware, ransomware and other cybersecurity threats.

Make no mistake: strong executive support can mean the difference between the company not recovering at all or coming back stronger and more respected than before a breach

What happens in the hours, days and weeks after that news leak will set the stage for how the company will survive. Proper handling by your security team will set the tone for remediation and proper handling of communications will set the tone for customers and consumers. The most important element in the handling of a cyber event is the response and support of your executive sponsor.

Learn the responsibilities and accountabilities that are bestowed on the various staff levels before, during and after an event. Jail time is a large motivating factor for any senior staff member. With or without the possibility of prison, having your personal name associated with a breach is not considered a smart career move.

Make no mistake: strong executive support can mean the difference between the company not recovering at all or coming back stronger and more respected than before a breach. Never waste a good crisis to ask for additional budget.

Scope and assets

Once you have your executives on board, the next step is to define the scope of your program and your inventory of assets.

Scope will include the entire company at some level, but you may have a scope for internal resources, one for customer resources, one for third-party resources, etc. Scope may be defined in terms of technology or business, application or process, people or buildings. Your executive sponsor can help define the scope of the program and your cybersecurity professional must help the executive sponsor understand the depth and breadth of the scope requirements.

Inventories may be tracked in simple Excel spreadsheets, maintained by accounting, or be tracked in sophisticated asset-management software applications that include automated discovery and tracking mechanisms. Regardless of if the starting inventory is simply hard assets (desk or desktop) or soft assets (operating systems or data), this inventory is a fundamental requirement for the security program. Without it you don't know what needs to be protected.

In your inventory, you need to include a careful accounting of all people, processes, technology and data. Use business processes to ease the tracking of assets. A lifecycle view of the beginning, middle and end of each asset class helps understand where and how data is collected, what it is stored on and backed up to, who has access to it and when.

For example, your human resources department holds a tremendous amount of data in the asset class of your people. The HR team is involved in the processes of recruiting, hiring, on-boarding and other actions during employment, such as performance reviews, transfers of employees to different roles and responsibilities and end-of-employment actions around terminations. Walking through these process-based lifecycles is a good method to acquire information about all data collected, what software or human method is used to collect the data and where the data is stored. Prepare to ask more than just the HR team for this information, as they will most likely not know what system their software and data is stored on.

There are many process flows that need to be mapped through your systems. Using basic interview styles with personnel in each department, you can uncover hidden gems. Talk to your financial department for possibility of credit cards being accepted, talk to sales about customers that potentially send data directly to them, talk to marketing about underlying Web pages that make up the website for the company. These processes are, or should be, documented in policy and procedure; don't forget to include all this documentation in your inventory.

Your system development lifecycle for all hardware and software is usually a vast asset classification. Inventories must include details such as:

- Operating systems – versions and service pack levels, database management systems, Web services and each piece of hardware's basic operating system
- The services running on the servers – include ports that are open and those that are explicitly locked down
- Firewalls and each network appliance – versions and service packs
- Wireless systems, phone and fax systems, security cameras, door access control systems, etc.
- Point-of-sale systems, including the use of apps and devices like Square
- Regarding apps, you'll need an inventory of all apps on each company device
- Don't forget to catalog any open source software within your organization

For a proper inventory, you need to know every data element associated with each of these assets and the lifecycle of that data element. Remember that data is the primary target for cybercriminals.

You have to know what data you have, and where it lives, to protect it.

You have to know what data you have, and where it lives, to protect it.

Framework and controls

Fortunately, depending on the industry your organization belongs to and the type of data you need to protect, your framework could already be set by outside standards. For instance, if you accept credit cards you must comply with PCI. If yours is a financial institution, FFIEC is your ruling standard. If your organization handles medical information, HIPAA will provide a set of standards and oversight.

If you don't already follow a regulatory standard, choose a general security framework like one of the following:

- ISO – Well-known international set of standards
- NIST – Established US standards that are required by federal agencies
- AICPA – Familiar auditing standards for service organizations
- CSA – Standard directed to cloud service organizations

Understanding regulations related to privacy of information is a special area, and a critical one, as there are a multitude of privacy laws throughout the United States and all around the world. If your organization handles international data you need to be aware of General Data Protection Regulation (GDPR), which replaced the EU Data Protection Directive. Privacy Shield provides the standard for protecting EU data which takes care of the countries in the European Union, but there are so many more countries that need to be considered if you store data from those countries.

Controls for any of the frameworks are built into your policy and procedural documents that support the overall organization creating a common strategic governance profile for the company.

All of these different laws, standards, regulations and provisions mean that if you have a breach of personal data, you will most likely need an attorney who specializes in privacy law.

Program development

Each business is unique. Each of the frameworks has many controls that are the same. Use the unique qualities of your business and the similarity of the various controls to build a program that meets your specific business objectives and needs. After reviewing the frameworks, you'll see that the following groupings of controls works well together. This is simply one example and you may find a different grouping will work better for your environment.

- **Governance** includes defining the policy and procedures and ensuring the organizational structure is in place—including executive sponsorship. This is the *Plan* phase of the PDCA model. These plans are incorporated into each of the different areas of the framework.
- **Asset management** goes back to your scope and asset inventory. This full discipline ensures all areas of the company have been identified.
- **Risk management** is of course assigning a risk to each of the asset categories, and is a full discipline itself.
- **Building security in** means you start from the beginning to build security into your systems acquisition and development process; into training and awareness; and into physical and environmental security requirements. Building security into all aspects of the business is more cost efficient than bolting security on after the fact. However, if security was not a consideration at the beginning, bolting on is what must be done.
- **Secure operations and maintenance** refers to the day-to-day running of the systems that we have built or contracted for. This is the *Do* phase that uses the *Plans* in the PDCA model. This includes all disciplines needed to keep the business running.
- **Continuous monitoring and assessment** includes monitoring activity of employees in their roles, external connections to the systems, the systems in their performance, and the performance against the goals or KPIs that were set in the governance areas. This is the Check phase of PDCA model.
- **Incident management** is a separate discipline that ensures that when the bad thing happens, you are prepared to respond. We discussed this area in a previous webinar and is covered in a brief that is available online. Your incident management team can mean the difference between the company surviving—or not.
- **Continuity management** is the area that is responsible for keeping the lights on in the event of any type of business outage. In this vast arena, knowledge spans all of the areas discussed and includes knowledge of the priority of recovery. This team works very closely with the incident management team at time of event.

> Governance, risk, compliance and privacy are each unique disciplines, yet they all work together to protect the business.

Identify roles and responsibilities

As mentioned earlier, to many organizations, security is associated only with the technology side of the business. However, for true cybersecurity you have to look at your organization as a whole. You'll want a

central team to manage your program that may include roles like:

- Chief security officer (CSO)
- Chief information security officer (CISO)
- Business unit security officer (BUSO)

Governance, risk, compliance and privacy are each unique disciplines, yet they all work together to protect the business. These disciplines work directly with other business disciplines for specific program activities: legal, human resources, marketing, finance, etc.

There are many specialized technology security profession disciplines that focus on the details of application security, network security, system security, forensics and more. The field is vast and growing.

Build policy

To build out your documentation for the program, you will inventory the controls needed to support the regulation or standards you are adopting. Some of these standards clearly define where you need a dedicated policy and supporting documentation.

Review your standard and decide how many documents you will need to develop, how many pages per document, how much detail in each document, and what document classification to use.

Policies are in general high level, but specific enough to define controls, whereas procedures are more detailed and discuss how to accomplish the control. Use different styles here—checklists, playbooks, runbooks—whatever will provide the level of detail needed. Keep in mind that while you may have a very seasoned employee that generally performs these actions, they still may need reminders at critical times to ensure they are performing all actions in the required order, and new employees will naturally need additional detail.

Determine your level of comfort in sharing these documents outside of your company. Creating a specific set of documents that are customer facing is good way to ensure the customer can see what they need for their due diligence, without sharing so much that you make yourself vulnerable to attack.

Awareness and training

The only way to ensure that jobs get done right is to educate the people that need to do the jobs. In other words, training is integral to any program.

We've all been through the annual awareness training, where we sit and listen to, or read, the information on the screen and pay enough attention to click through the test if there is one. Your participation can then be checked off, but did you really learn anything?

Tabletop exercises and real-life scenario-based tests are great; the more everyone practices, the better their performance during day-to-day activities or an actual event.

Role-specific training can be helpful as a way to make a more lasting impression. Ask developers to take specific security-related training in the language and platform they code in, and provide a different training for your customer-facing employees. Employees that handle sensitive data like employee data and payment data need specific and focused training to understand their importance in the bigger security posture.

Follow training with actual tests and exercises to give employees the practice they need. Tabletop exercises and real-life scenario-based tests are great; the more everyone practices, the better their performance during day to day activities or an actual event.

Operationalize

The more your staff knows what is expected of them, the more efficient and productive they can be. Use the procedural documents mentioned earlier—runbooks, checklists and playbooks—to walk through each role. This will confirm the accuracy of the documents and ensure the full job gets done.

All employees should have a goal in their annual review to test security skills, such as being able to properly identify an event and report it to the right authorities. They should show awareness of each of the steps they are required to perform as day-to-day activities in the name of good security.

Specific technical resources are required to monitor for events. Tools can automate many of these functions, but they can't automate them all. New vulnerabilities are discovered daily, just like anti-virus programs that have daily updates, your monitoring tools and configuration should be updated as well.

Continue to review and improve

This takes us back to where we started, with Plan-Do-Check-Act. Create a committee that can review the security posture, focusing specifically on gaps to controls or vulnerabilities found, and define a remediation plan for all. This continual improvement process is a required part of your framework. Use this process to ensure your business leaders are aware of the security posture, especially as areas that need attention that may be in their area of responsibility.

Policy documents should be reviewed regularly by a governance board or security committee. Specific attention to policy documentation must be done out-of-band for any major changes to the business, as well as immediately after an event occurs.

Five common sense security principles

After all this discussion on your cybersecurity program, what about the common-sense principles? These principles should be ingrained into your overall cybersecurity program.

Principle #1: Locked Door

You lock your home—now lock your network. This means having a reliable and secure data center and following basic safety rules, like locking down ports, shutting off services, removing rights and privileges when no longer justified, and using firewalls. You'll also need host and network intrusion detection and prevention (IDS/IPS) as well as using physical access controls such as badge, PIN pad and biometrics etc., to ensure you let only the right traffic and the right people in.

> The best way to keep a secret is to encrypt it.

The best way to keep a secret is to encrypt it. But what to encrypt? Encryption can occur at many layers—the network, the physical disk drive, the database, or individual fields. Encryption can be inherent to the component, or added as an additional layer within the application. All encryption is not the same. Algorithms have different key lengths, some are slower in performance than others and some have been compromised through the ages. Be aware, and keep current with encryption techniques.

At the application layer, strong authentication is key. Create a process for good passwords and keep it simple so people will use it, but make it strong to keep the bad guys out. There are various mechanisms being used and created for identity proofing, with user ID and password combination the most widely used. Passphrases, account ID images and challenge questions are other techniques. A simple technique to use for challenge questions is to not respond with the answer to the question being asked. If the question is "What is your mother's middle name" use a word like "chair" or "fish." These red herring responses cannot be traced back to your Facebook account or other social accounts.

Remember that malicious insiders are also a threat; you must watch your watchers. Monitor systems to know what your staff is doing and ensure key functions are properly segmented—and that there are enough of the right hands at the right place to prevent collusion.

Principle #2: Defense is the best defense

You defend yourself—do the same for your network. Basic defensive tools include anti-virus and anti-malware. These should be present on any device that can be connected to the Internet. Just know that these are defenses against known bad actors, not upcoming unknowns; the new wave of zero-day threats must be defended with a different strategy.

Consider tools that prevent your end users from installing anything that is not a known good. By removing administrative rights and privileges from the end user, allowing only the corporate standard set by IT security, by removing the ability to plug in any device to a USB, HDMI or other available ports on the system, by preventing the end user from browsing to any website they desire, by preventing users from sending any file they want via unsecured email, and by faithfully teaching to each user in the manner they need to be taught, you can make huge strides toward true protection.

Keep software up-to-date to ensure vulnerabilities that have been patched by the vendor are patched in your environment.

Principle #3: Shiny new

We all like new tech toys, but at the same time, we resist change. This desire for the latest and greatest, and yet not wanting to move forward with progress, is something to be aware of in the cybersecurity sphere.

The shiny, new rules are basic: If you installed it, update it. Keep software up-to-date to ensure vulnerabilities that have been patched by the vendor are patched in your environment.

If you did not specifically search for a topic online, yet a link to a topic is presented to you, ignore it. Cybercriminals create targeted topics as clickbait to lure you down a path to malware.

If it's too old for the owner/manufacturer to update it, it's too old for you.

Update and change passwords, security questions and other features of identity-proofing frequently.

Principle #4 Minimalism

Whatever you have, chances are you don't need it all. You don't need all the data you may be asking for, or for that matter, giving out. Medical forms often ask for Social Security numbers, though there are few cases where a medical facility needs that information. Many forms ask for a driver's license, though they have no need for that information.

Conversely, companies don't always think through the data they collect on their websites, in their products or from their employees. You really don't need multiple copies of all data, but you do need redundancy and a good backup. Know where all your data resides; if you don't need it, get rid of it. Don't ask for stuff you really don't need and keep data for only as long as needed.

Principle #5: Eyes wide open

Privacy can be defined in many ways but usually includes the right to be left alone and the right to control information about oneself. But with the success of social media, all of that has changed. An astonishing number of people feel comfortable posting intimate details of their private or professional life on these sites that they would never have revealed years ago.

By gathering a few data points from one social site, and more data from another and so on, cybercriminals can paint a highly realistic picture of a person's activities.

The fact is, cyber space is cyber perpetual; whatever you put in the cyber world is there forever. Open your eyes to this concept and reevaluate which data you are storing, where you are storing it and how much security is wrapped around it. Should this particular data be stored in this manner? Is it all properly documented? And is it permitted by policy?

Employees must be trained so that they really understand the administrative policies of your company. Not every administrative policy will have a technical policy to back it up, though eventually many, if not most, will. You can't write an administrative policy to cover everything, and you can't control everything an employee does; that is why training is vital.

Training should be specific to each employee's role. Customer-facing employees will receive different training than your IT staff, though all employees must receive corporate training about all policies they need to adhere to. Employees must be required to acknowledge that they have read and understood the policies. Part of cybersecurity training is simply showing employees how to make the right decisions, or how to know when to not make a decision. In many cases it's better if you remove the choice completely so that there is no option to make a wrong decision.

Keep an eye on your networks, systems and applications. Use audit logs to capture who logs into and out of systems and the activity in between those two functions. Log management is a discipline that requires a specific talent as logs must be secure from tampering. You must define a method for log review, preferably using an automated security event and incident management tool, (SEIM). Monitor your employees from the beginning by having background checks performed prior to employment.

There are a variety of ways to perform assessments. Each framework may have an assessment component as part of the package. Some other commonly used third-party assessments include Shared Assessment Program and their data collection tool affectionately known as a SIG (standardized information gathering). Another is CAIQ (the Cloud Security Alliance (CSA) Consensus Assessment Initiative Questionnaire), which provides a standard set of questions that can give you reasonable assurance of the security posture of your company.

Vulnerability assessments or vulnerability scans for your network and systems should be performed on a regular basis, typically weekly, to keep the perimeter wall managed. Application assessments are dynamic and are performed against the external website, whereas static assessments are performed against the code base. These should be performed regularly as well. For static assessment, many development teams have plugins that perform security debugging within the IDE. This is a great way to manage security vulnerabilities from an early stage of development. The earlier a vulnerability is discovered, the more economical and efficient it is to correct.

Process-based assessments include the likes of the PCI Security Standards Council, which provide a common set of questions that must be responded to, based upon the tier within the credit card acceptance in combination with standard and regular network vulnerability tests.

It's a good idea to employ a third-party company that specializes in security assessments to perform audits to standards such as ISO 27001 and 23001, or AICPA audits to SOC 1/SSAE16 for financial statements, or the SOC2 for Trust Security Principles of Confidentiality, Process Integrity, Availability, Security and Privacy. These reports go a long way to provide customers assurance of the security posture of the company, and can help divert additional scrutiny of customer specific audits.

DRJ (Disaster Resource Journal) provides an excellent resource that provides over 100 rules and regulations that are inclusive of business continuity and security. You can find that here: http://www.drj.com/resources/dr-rules-regulations.html

Summary

As a business continuity professional, you have a unique set of skills that can help your company's cybersecurity professional ensure proper coverage where needed to collect information and ensure it is documented, repeatable and auditable.

Spread the word through awareness training and educational opportunities. This can be done through lecture-based training, via webinars or by using other communication channels like automated alerts, text messaging, emails and phone calls.

Ultimately your goal is to ensure the overall resilience of your company; with this in mind, getting cooperation and collaboration should be an easy sell between departments.

Use the PDCA or a similar management model to get the support of the executive management staff. Use your common business goals to get cooperation with the different teams and business units. And while you may tailor one of the many standards to your specific needs, use as much of the standard as possible. These have already been tested by many organizations and are known to be effective.

Follow the common-sense principles, or define your own if that works better for your company. Make security just another part of life and the day-to-day expectations of the organization.

And finally, communicate. Get the message out early and often, make it as accurate as possible—but don't let perfection stand in the way of progress or communication. Whenever possible, use an automated notification system so that you can get your messages out by every possible means.

This paper was written by Cheryl Carmel. Ms. Carmel is a member of (ISC)², where she holds her CISSP and participates in the Safe and Secure Online cybersecurity youth education program. She also belongs to the International Association of Privacy Professionals, where she holds her CIPT (CIPP/IT), and is a member of ISSA, OWASP and InfraGard.

For more briefs, white papers and other helpful resources, visit: onsolve.com

The Common Sense Rules of Cybersecurity on next page

About OnSolve

OnSolve is the market leader in real-time, mass notification and collaboration solutions used by the world's largest brands and thousands of government agencies to deliver critical information in any situation. Mass notification and collaboration is an essential element of emergency response and business continuity planning, keeping teams on track and coordinating during critical events. The OnSolve suite of critical communication tools is a key component of the business continuity, emergency response, IT alerting, employee safety and security programs of every organization we serve. Visit us on the Web at www.onsolve.com.

The Common Sense Rules of Cybersecurity

1. Don't let the fox in the henhouse – maintain a separation of duties.
2. Always watch the watchers – prevent collusion.
3. Always maintain a good backup.
4. Don't believe everything you are told – trust but verify.
5. Always be reachable, and keep your systems reachable.
6. The best way to keep a secret? Encrypt it.
7. Never waste a good crisis to get additional budget.
8. Never take security for granted.
9. Never go anywhere without a crash kit.
10. Always involve legal counsel when a data breach is concerned.
11. A breach through the front door is bad; a breach from the back door is scary.
12. If everyone else is wrong and you are right, it's time to rethink.
13. The "opts" have it. Respect individual's choice with opt-out options.
14. If you find a hole – plug it.
15. If the moat has been breached, change the keys to the castle.
16. Personal data is more valuable than gold or rubies – value it and protect it.
17. Personal data is currency – value it and protect it.
18. The purpose of a password is to identify you, as you, and you alone.
19. Patent leather shoes reflect up – don't expose valuable resources.
20. Don't give keys to the castle if all that's needed are keys to the stable.
21. Use phobias wisely – be clickaphobic and linkaphobic.
22. Don't lose stuff.
23. If you need it – keep it safe.
24. If you don't need it – get rid of it, completely.
25. If you installed it – update it.