WHAT GOOD CYBERSECURITY REALLY MEANS

And How to Implement it at Your Company

WHITEPAPER

What Good Cybersecurity Really Means
And How to Implement it at Your Company

Adapted from Otto Aulicino's three-part LinkedIn article series. The originals can be found here, here and here. Otto is WatServ's Director of Information Security.

Table of Contents:

Introduction

Billions of records are compromised every year in data breaches, and the average cost of a mega-sized data breach was US$3.86 million, according to IBM's Cost of a Data Breach report.

High-profile incidents not only cost money to recover from, but they have also brought a question to the forefront of the public's attention: What exactly is "good" cybersecurity? For business leaders and security professionals, this has translated to: How can we ensure our organization has the right amount of cybersecurity measures in place?

Although technology is constantly evolving and needs vary vastly depending on industry, organization size, and so on, this whitepaper offers a definition of what constitutes "good" cybersecurity and outlines some of the fundamentals a business should have in place in order to have confidence in their security programs and systems.

No company wants to be the next bad news headline. However, with so many conflicting opinions on what is required to achieve an ideal cybersecurity posture, this whitepaper guides readers through the process of defining "good" cybersecurity within each unique context.

Recent publicly disclosed breaches indicate that, in many cases, simple solutions could have prevented the breach or reduced damage from it. This is the case for both the Facebook and Burger King breaches in 2019.

What is “Good Cybersecurity”?

When it comes to cybersecurity, much is said (and a lot of it at a very high level) about what organizations should or should not be doing in order to protect themselves.

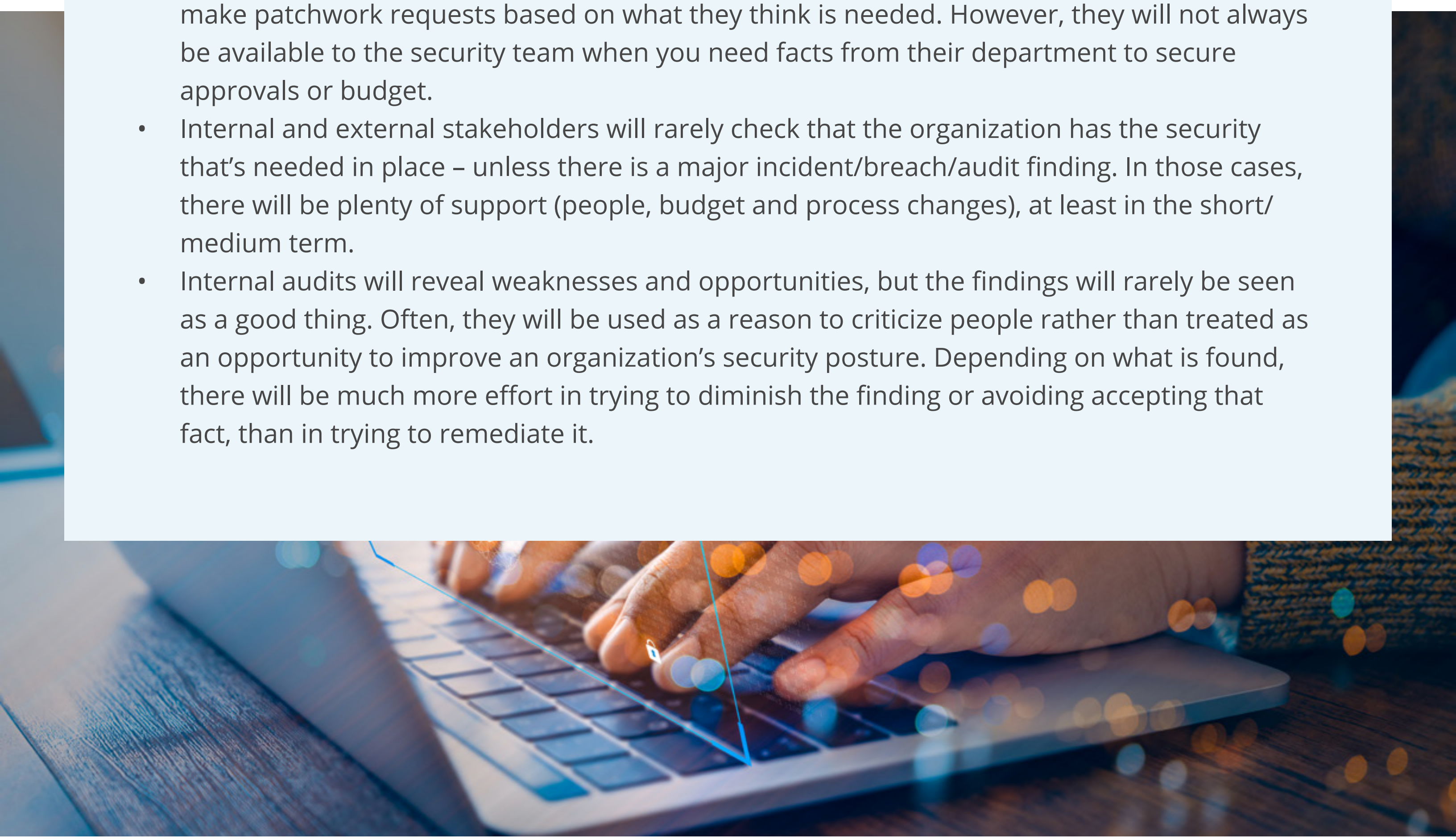
But the truth is that at many of these same organizations, little is being done to help bring security (cyber, information, etc.) risks to a manageable level.

Why is this?

The problem – which will no doubt be familiar to anyone who has ever worked in cyber/information security – is that “everyone knows about security” without actually understanding the full extent of what they’re up against.

Here’s what cybersecurity conversations actually end up looking like in many organizations:

- Vendors try to sell you what they have, but their products aren’t necessarily what you need.
- Internal stakeholders want to demonstrate that they “know what needs to be done” and may make patchwork requests based on what they think is needed. However, they will not always be available to the security team when you need facts from their department to secure approvals or budget.
- Internal and external stakeholders will rarely check that the organization has the security that’s needed in place – unless there is a major incident/breach/audit finding. In those cases, there will be plenty of support (people, budget and process changes), at least in the short/medium term.
- Internal audits will reveal weaknesses and opportunities, but the findings will rarely be seen as a good thing. Often, they will be used as a reason to criticize people rather than treated as an opportunity to improve an organization’s security posture. Depending on what is found, there will be much more effort in trying to diminish the finding or avoiding accepting that fact, than in trying to remediate it.



So, while “everyone knows” about cybersecurity, there’s often a limited understanding of what a company is truly up against. This leads to scenarios where a company’s security strategy falls into one of the following categories:

“Using a bazooka to kill ants’ nests”:
You know that something needs to be addressed, but you spend a lot to do so in an untargeted way.

“Aiming your nerf gun at a troll without wearing your glasses”:
You have no idea what you need to address nor what you need to do so.

“Trying to find a target using your sniper rifle while blindfolded”:
You know what tool to use (and may even have it) but you don’t know exactly what needs to be addressed.

While every company is different and has their own reasons to act/react differently when it comes to cybersecurity, these standard approaches are less than ideal. To begin defining what good cybersecurity really means, organizations need to step back and focus on “security fundamentals” first.

Identifying Security Fundamentals

In order to understand what good cybersecurity means for your organization, you need to start with the fundamentals:

1. **Understand what needs to be protected:** Protecting your organization's information assets is the raison d'etre of a security professional. Without understanding what you need to protect, you will likely end up in one of the scenarios listed above. Whether it's the crown jewels or a pot of gold at the end of the rainbow, once you know what you need to protect (and where they are located), you can focus your efforts.
2. **Understand how your environments are architected:** You need to take a step back and understand your environment at a higher level. How are things connected? How are devices used in your organization? How does information flow? Knowing this is critical for addressing security concerns, especially when you are under pressure (for example, in the case of an incident).
3. **Understand best practices:** Awareness of cybercrime and ransomware cases have raised the profile of cybersecurity concerns. But if you only follow the news, your strategy will likely be all over the place. Instead, understand and use best practices (such as ISO 27001/27002 or NIST Cyber Security Framework) to do a simple gap analysis to determine where you are at and what needs your attention.

Once you have these fundamentals well-defined, you can use the knowledge you've gained to improve or remediate your security posture. This may include:

- Planning remediation activities related to any unacceptable risks you have identified
- Address any areas where you can make quick wins
- Improve on areas where efficiency gains can be made

Achieving these outcomes are the basis of a good cybersecurity program.

The precise blend of these three activities will be determined by your situation, your budget and your staff resources. But taking these steps forms the basis of a good information security program that protects your assets and is targeted to your organization.

Implementing an Information Security Program

In the previous section, we set out a definition of what good cybersecurity means, and some of the basic steps that you can take to ensure you have the fundamentals of good cybersecurity in place.

But if you're putting together an Information Security Program from scratch, you'll want to consider in more detail the critical components of an information security program, and what those components mean in practice for your organization.

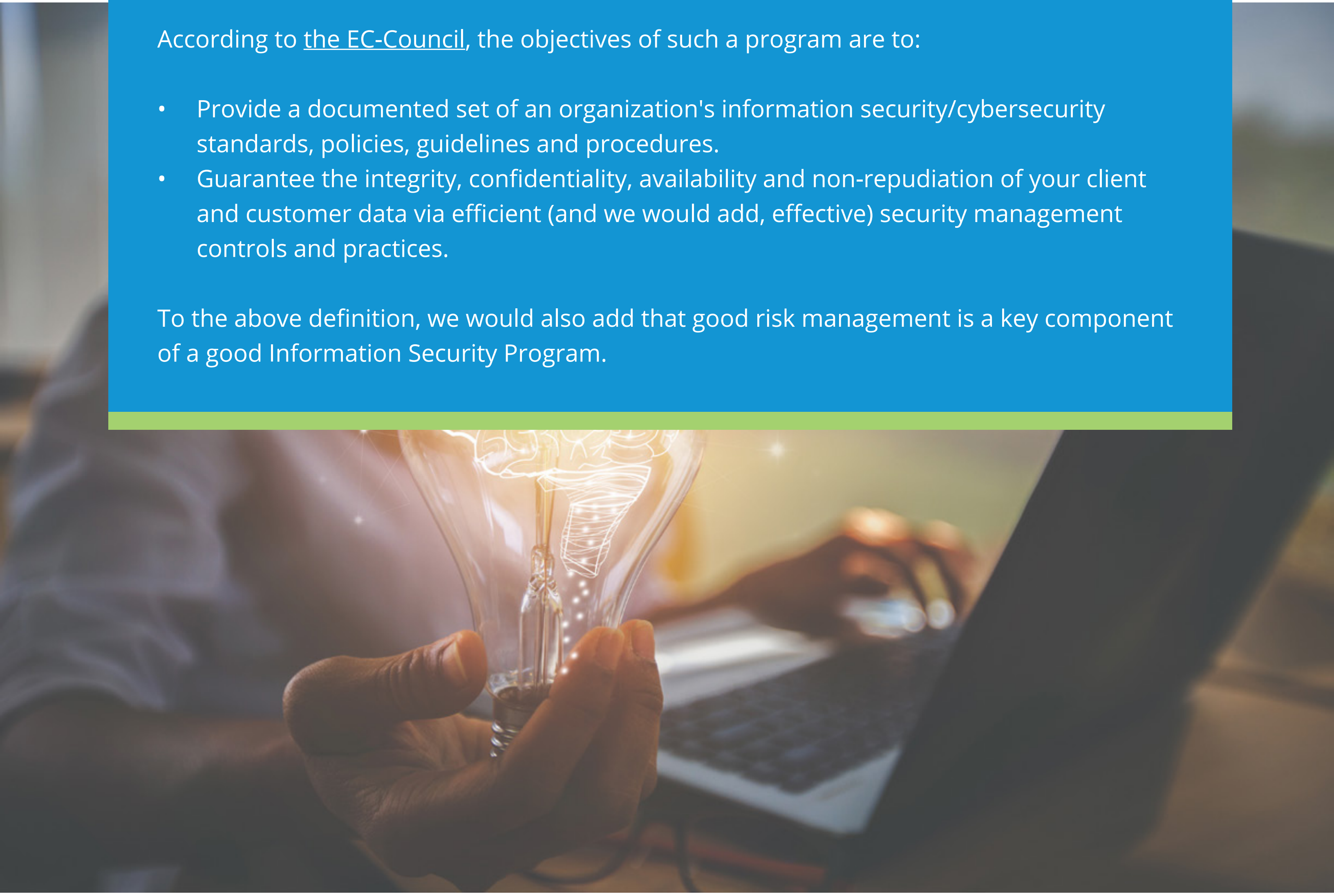
What is an "Information Security Program"?

To start, let's define what an Information Security Program is.

According to the EC-Council, the objectives of such a program are to:

- Provide a documented set of an organization's information security/cybersecurity standards, policies, guidelines and procedures.
- Guarantee the integrity, confidentiality, availability and non-repudiation of your client and customer data via efficient (and we would add, effective) security management controls and practices.

To the above definition, we would also add that good risk management is a key component of a good Information Security Program.



4 Critical Components of an Information Security Program

1. Risk Management

Let's start by looking at the additional pillar that we added to the EC-Council's definition of an Information Security Program: Risk Management. In Information Security, risk management refers to the process of identifying, evaluating and treating risks related to the organization's valuable information.

The reason we're starting here is because this should be the starting point for any CISO or head of security who is considering how to build out their Information Security Program.

Without good risk management, you won't be able to identify which tools you need, or the relevant importance of various aspects of your Information Security Program to your organization. For example, everyone knows that anti-malware is important and required in most cases, but without a comprehensive risk assessment, you will never be entirely sure if the anti-malware is more or less important than other tools, improvements, resources and so on.

In a world where you had an infinite budget, perhaps this wouldn't matter: you'd just buy the best of everything, for all scenarios. But, in reality, organizations want to understand how to prioritize their security concerns and maintain an efficient security program.

Once you have a comprehensive risk assessment in place, you can turn to the key components of an Information Security Program as identified in the EC-Council definition:

2. Policies

Policies should be the starting point for any Information Security/Cybersecurity documentation.

Your policy documents should provide the intent, overarching direction and governing principles for the organization's security efforts. This should ensure that appropriate levels of security, confidentiality, integrity and availability of information assets owned by or in the care of the company are applied accordingly.

The goals of creating your policy documents should include (but not be limited to):

- Setting out the approach to managing your information security objectives.
- Define your information security requirements in support of the organization's business strategy.
- Ensure compliance with applicable regulations, legislation, and contracts.
- Address the current and projected information security threat environment.

As a result, when an Information Security/Cybersecurity policy is well defined, it serves as the strongest pillar of the Information Security Program. However, it is very common for these policies to become a mere formality, so as you are implementing your Information Security Program, it is important that you seek and gain support at the highest levels of the organization.

At a minimum, these policies must be reviewed and approved by leadership, or this pillar will not be strong enough to support the program.

3. Standards

Cybersecurity standards are by far the most misunderstood type of documentation within an Information Security Program.

A standard is defined by BSI Group as “an agreed, repeatable way of doing something. It’s a published document that contains a technical specification or other precise criteria designed to be used consistently as a rule, guideline, or definition.” In theory, standards will elaborate and precisely define what and how a policy statement is implemented, whenever possible.

Here’s an example of how this might work within your organization. If a policy statement indicates that “incident response plans must be developed,” standards would provide the “what” and “how” of what the development of these plans should look like. This may include frameworks to use, templates, references, specific timelines, and others.

4. Procedures and Guidelines

Procedures and guidelines are sometimes used interchangeably. The main difference between the two is that procedures are mandatory and guidelines are not.

Procedures are a series of detailed steps that must be followed when accomplishing a particular task. You will often hear procedures referred to as standard operating procedure (SOP).

An example of a procedure is a ransomware incident response procedure. This procedure would outline the steps to be taken when a ransomware incident occurs. If a ransomware incident does occur, these steps **must** be followed.

Guidelines contain recommendations or suggestions that are not mandatory to follow. They are best practices that may or may not be followed depending on the context of the situation.

An example of a guideline is “email communication guidelines,” in which some recommendations are provided on how to communicate with a customer. The guidelines may contain best practices such as maximum number of recipients, words to avoid using, etc. However, if the situation calls for it, you can decide to ignore a guideline.

Information Security Controls and Practices

Finally, let’s look at the second part of the EC-Council definition of the goals of an information security program:

“the objectives of an information security program are [...] to guarantee the integrity, confidentiality, availability, and nonrepudiation of your client and customer data via efficient security management controls and practices..."

While it was relatively easy to unpack the first part of the definition (policies, standards, procedures, and guidelines), this is a little more conceptual and harder to digest. The definition includes the CIA triad (confidentiality, integrity, availability) and non-repudiation as goals of an information security program. The mechanism for delivering these outcomes is efficient – and we would argue even more importantly, effective – security management controls and practices. For the purposes of this whitepaper, we’ll focus on what exactly those effective controls and practices are and how they form another critical pillar of your Information Security Program.

One thing to note is that many highly visible aspects of your Information Security Program, such as Awareness and Training efforts or Identity and Access Management, can be considered under the umbrella of Information Security Controls and Practices. While this may cause some debate among professionals, our contention is that these methods are all either forms of controls or practices that have the aim of controlling risks to the organization.

1. Information Security Controls

Information Security Controls are the most effective way to respond to risks identified in the organization, as they are generally not one-off activities.

The controls that you establish within your organization will happen continuously according to a predefined frequency in order to ensure that risks are kept within acceptable levels.

Controls may fall into one of three categories:

- **Detective**: Controls that are designed to detect errors or irregularities that may have occurred (for example, a malware scan report review to make sure nothing is missed by your information security practices).
- **Corrective**: Controls that are designed to correct error or irregularities once they have been detected (for example, applying out of band system patches, quarantining viruses or rebooting a server).
- **Preventive**: Controls that are designed to keep errors and irregularities from occurring in the first place (for example, access controls or approval process for special transactions).

Another way of controlling risks is to avoid the risk altogether, but that falls outside the parameters of this discussion.

2. Information Security Practices

Information Security Practices (and we can include processes here, too) are the actions you take as part of your Information Security program that aren't controls.

To understand the difference, let's look at one of the examples from the previous section.

In this scenario, your organization has established a "malware scan report review" control.
The processes or practices that correspond to this control would be your regular anti-malware management (which might include, among other things, running regular malware scans and quarantining malicious files whenever they are flagged).

If this routine process works well, the malware scan report review control will not catch anything. However, if for any reason the malware scan wasn't able quarantine the malware, you would be able to act on it at the time the control flagged it.

How to Avoid Common Gaps in Your Information Security Program

Now that we've discussed the fundamentals of what an Information Security Program is, let's look at some of the common gaps that arise in Information Security Programs.

Using Information Security Controls Frameworks to Identify Gaps

We mentioned above the importance of using an Information Security Controls Framework as a critical step in getting your security fundamentals in place. These frameworks can also help you identify gaps in your existing program. You may use a single framework or multiple frameworks, but it is important to use at least one.

The exact choice of which frameworks you use will be dependent on factors such as regulatory compliance, company alignment to specific standards, technology requirements (e.g., cloud vs. on premises implementations) and so on.

Here are some of the common frameworks used by security professionals, although this is not an exhaustive list:

- Center for Internet Security (CIS) Controls: The 18 CIS Controls (cisecurity.org)
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM): CSA (cloudsecurityalliance.org)
- Control Objectives for Information Technology (COBIT): COBIT | Control Objectives for Information Technologies | ISACA
- NIST Cybersecurity Framework (CSF): Cybersecurity Framework | NIST
- International Office of Standardization (ISO) 27001: ISO - ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements
- International Office of Standardization (ISO) 27002: ISO - ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls

8 Common Gaps to Check For

Gaps will often be identified when undertaking a comprehensive risk assessment for your organization. However, some common gaps can slip through even the most rigorous risk assessment, either because something is missing entirely from a security program or because it has been implemented but at a very low level of security.

Here some of the most common gaps, so that you can check your own program for them:

1. Asset Management

Asset management is one of those “hot potato” responsibilities in many organizations. It is rare for there to be a single dedicated unit for asset management, which means it often exists across different parts of the organization (or perhaps not at all).

When you ask the question “who is responsible for asset management in our organization?” you may hear one of these very common responses: “it depends,” or “what do you mean?” or the dreaded, “I don’t know.” If you encounter some variation of these responses, you likely have an asset management gap.

While it's not the role of the Information Security Program to implement asset management processes and tools, your program should work with other teams to implement or fix asset management within the organization, so that you have visibility into what needs to be protected.

2. Sensitive Information

Similar to asset management, there is often a lack of awareness within organizations about what sensitive information is being held and where. Knowing where these sensitive information assets are is critical in order to adequately protect them. Sensitive information assets should be considered the “crown jewels,” and so require rigorous protection around them.

In theory, if you have a good Information Classification scheme, it shouldn’t be too complicated to address this gap. You may be able to use monitoring mechanisms to identify where such information assets are (e.g., scanning for metadata on file shares) as well as how and if they are being moved around (e.g., data loss prevention tools or cloud access security brokers).

While the costs of these tools may outweigh the benefits for your organization, the absence of these tools should not deter you from closing your sensitive information gap. This is a critical part of ensuring that your organization has the security it needs.

3. Security Monitoring (Scope Gaps)

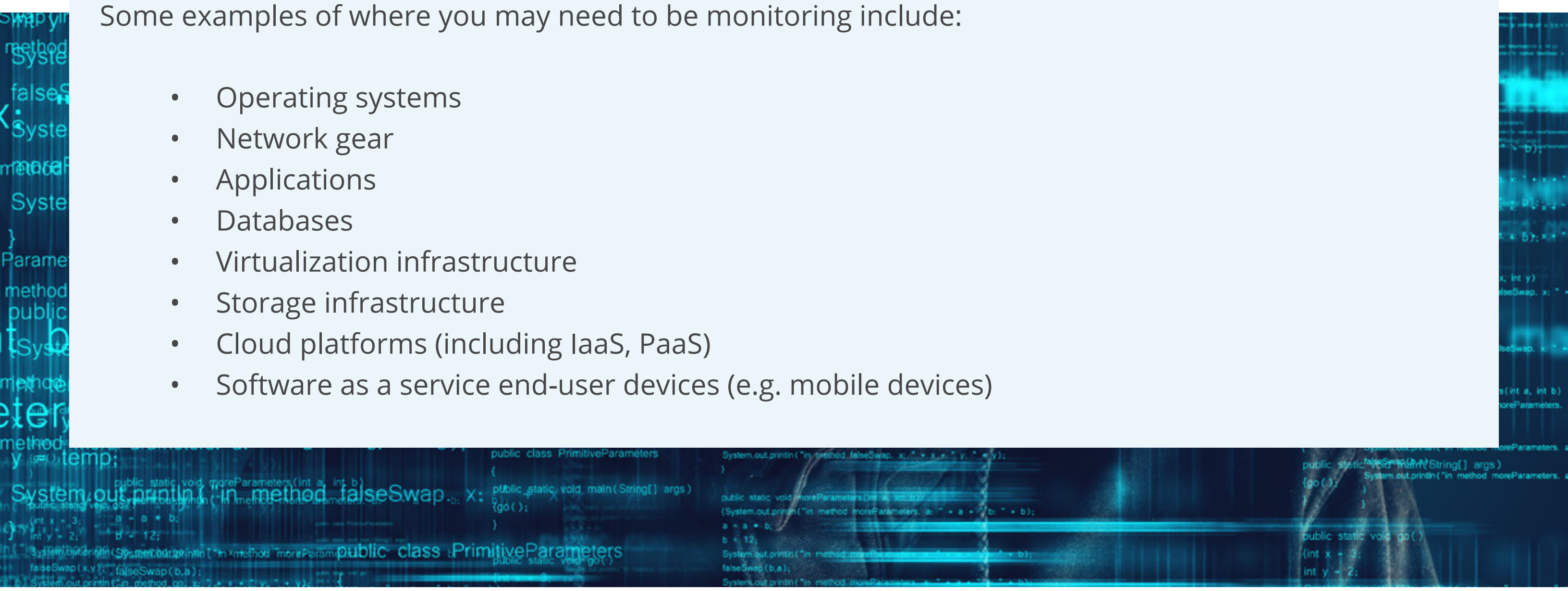
You may be surprised to see security monitoring on this list, as most companies have some type of security monitoring in place.

However, it is common for security monitoring to be implemented based on the expertise of those in charge. So, for example, if a former network engineer is now head of security at your organization, it is likely that security monitoring will be placed on network traffic or gear. The same can happen for leaders whose expertise lies in application development, operating systems, etc.

However, a comprehensive security monitoring system shouldn't be based on the particular expertise of an individual, but rather on monitoring what needs to be monitored. Of course, the definition of what needs to be monitored will differ from company to company. As a rule of thumb, security monitoring should strive to identify security threats that could lead to security events such as potential or actual security incidents. The point of performing security monitoring is to protect the organization before an incident happens, as well as identify incidents as they materialize. This allows you to take actions to remediate and, in the aftermath, perform digital forensics analysis.

Some examples of where you may need to be monitoring include:

- Operating systems
- Network gear
- Applications
- Databases
- Virtualization infrastructure
- Storage infrastructure
- Cloud platforms (including IaaS, PaaS)
- Software as a service end-user devices (e.g. mobile devices)


public class PrimitiveParameters
System.out.println("in method falseSwap. x:
public class PrimitiveParameters

4. Incident Response Preparedness

NIST defines a security incident as: “An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.”

The high-profile security incidents that you have no doubt seen in the news such as ransomware attacks or persistent threats can look like something out of a Hollywood movie.

It can be hard to believe that your organization could ever suffer such an incident – and of course, the hope is that your security program will indeed prevent them from happening in your environment.

However, as the adage goes, hope for the best, plan for the worst. Security incidents are some of the most challenging situations for security professionals to manage and preparing for them can help you respond more effectively when or if an issue arises.

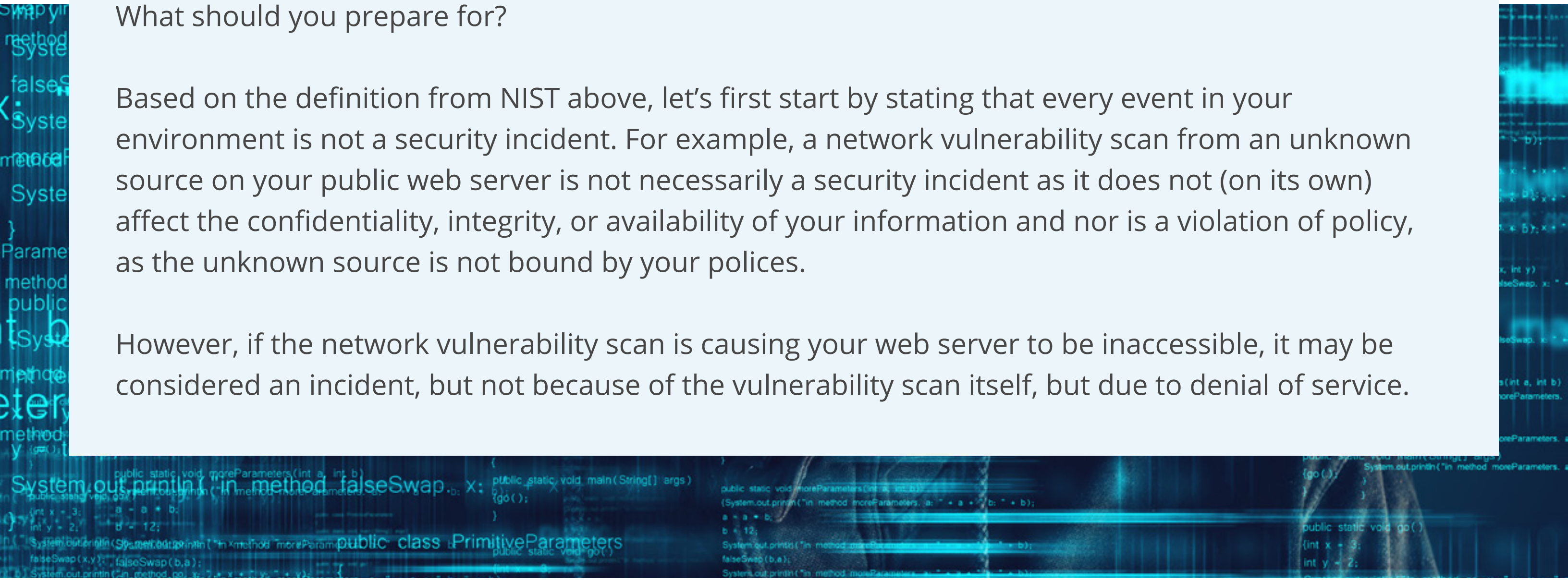
Incident response preparedness involves:

- Recognizing which incidents are more likely in your environment.
- Understand which types of incidents would have the most impact on your organization.
- Ensuring readiness to respond to incidents in a standardized manner to ensure that damage/impacts are reduced to minimum.
- Willingness to test your incident response plans or playbooks regularly.

What should you prepare for?

Based on the definition from NIST above, let’s first start by stating that every event in your environment is not a security incident. For example, a network vulnerability scan from an unknown source on your public web server is not necessarily a security incident as it does not (on its own) affect the confidentiality, integrity, or availability of your information and nor is a violation of policy, as the unknown source is not bound by your polices.

However, if the network vulnerability scan is causing your web server to be inaccessible, it may be considered an incident, but not because of the vulnerability scan itself, but due to denial of service.



Bearing this distinction in mind, you can start considering what types of incidents you want to be prepared to respond to. As a rule of thumb, you should have responses prepared for the incidents that you consider to be the most probable and most impactful threats to your organization. You should have plans in place to respond to "the unknown" at a high level.

Here are some of the most common types of incidents organizations need to prepare against:

- Ransomware
- Malware outbreak
- Identity compromise
- Denial of Service
- Unauthorized Access (to systems or data)
- Data Loss/Theft and Data Leakage
- Phishing

Note: this is not an exhaustive list, but rather a starting point for you to begin defining your own incident response playbooks, plans and resources.

5. Incident Response Post-Mortem Analysis

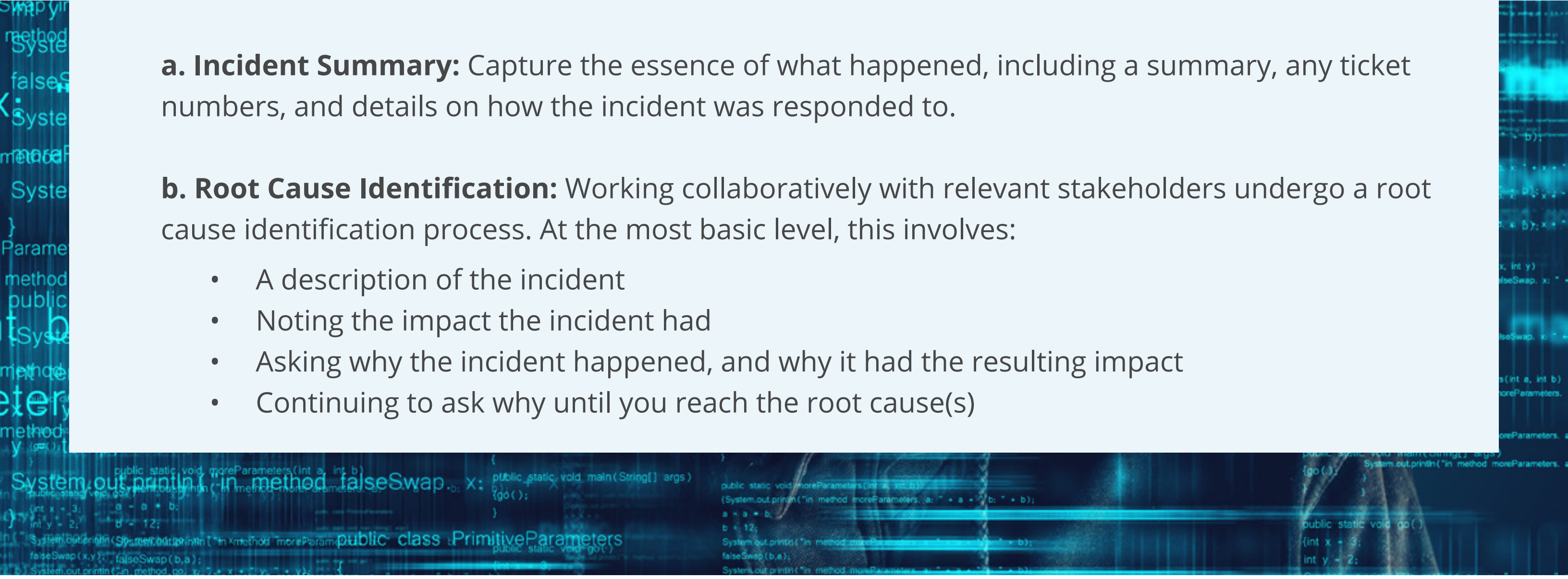
This is another item that is commonly missed, mostly because it is easily taken for granted. In the wake of an incident, you may hear a common refrain of "lesson learned, we know what to do next time." It's less common, however, for organizations to undertake a formal process to review incidents, what led to the incident, how to improve the organization's security posture and changes need to avoid future incidents.

Here are the steps we recommend be taken in any post-mortem analysis process:

a. Incident Summary: Capture the essence of what happened, including a summary, any ticket numbers, and details on how the incident was responded to.

b. Root Cause Identification: Working collaboratively with relevant stakeholders undergo a root cause identification process. At the most basic level, this involves:

- A description of the incident
- Noting the impact the incident had
- Asking why the incident happened, and why it had the resulting impact
- Continuing to ask why until you reach the root cause(s)



c. Document the root cause(s): Note the final root cause of the incident, the thing identified that needs to change to prevent this class of incident from happening again.

d. Backlog check: Verify if you had plans to address the root cause, or if there was any unplanned work that could have prevented this incident, or at least reduced its impact. A clear-eyed assessment of the backlog can shed light on past decisions around priority and risk.

e. Recurrence: Identify any other previous incidents that can be attributed to the same root cause. If there are, note what mitigation occurred in those cases and question why the incident was able to occur again.

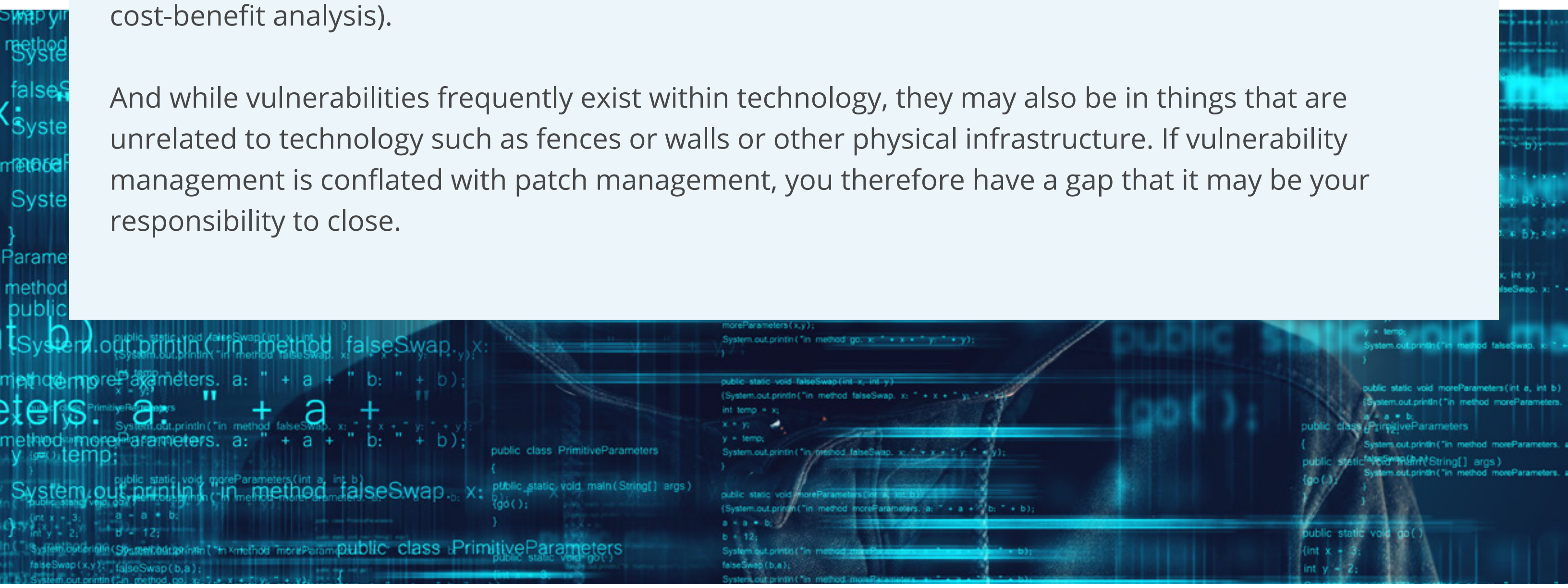
f. Document Lessons Learned: Discuss what went well in the incident response, what could have been improved, and where there are opportunities for improvement.

g. Create Action Plans: Describe the corrective action ordered to prevent this class of incident in the future. Note who is responsible for each action, when they must complete the work, and where that work is being tracked.

6. Vulnerability Management

Vulnerability management is commonly bundled in with patch management, making it easy for a gap to occur. Managing vulnerabilities means identifying your vulnerabilities and taking the appropriate steps to remediate them (which may include accepting some vulnerabilities based on a cost-benefit analysis).

And while vulnerabilities frequently exist within technology, they may also be in things that are unrelated to technology such as fences or walls or other physical infrastructure. If vulnerability management is conflated with patch management, you therefore have a gap that it may be your responsibility to close.



7. Privilege Management

There are many gaps that can occur within the realm of Identity and Access Management, but Privilege Management gaps are some of the most common.

To understand why this gap is so critical to close, let’s define the difference between a permission and privileges:

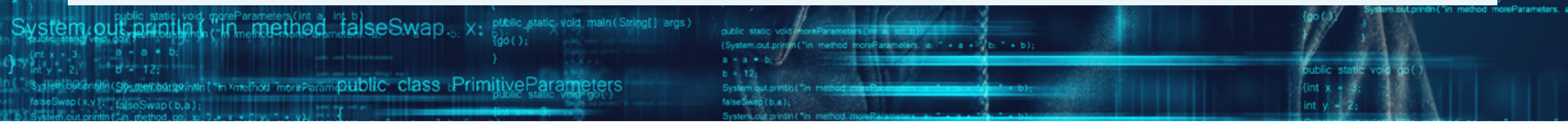
- A **permission** is a property of an object, such as a file, user account, server etc. The object itself will list what (e.g., user account) is permitted to use the object, and what they are permitted to do (e.g., read, modify etc.).
- A **privilege** is granted to users, roles, or groups that governs how they can interact with objects such as files, servers, etc. Privileges create the means for a user or role to globally perform actions that are not ordinarily available such as provisioning a new server or creating new user accounts.

Managing privileges is therefore extremely important to ensure that no one can perform these actions globally unless doing so is an expected part of their role. Even where a role may commonly perform certain actions, certain privileges must be secured and used only when necessary through requesting “just-in-time” privileges.

8. Secure Configuration/ Benchmarks/Hardening

As more and more organizations migrate to the cloud, it is easy to think that these gaps are up to your cloud service provider to handle. However, there are many different models for how cloud services are provided, including software as a service, platform as a service and infrastructure as a service. It is important to know what responsibility your organization has to “harden” your set up, otherwise you risk falling into the gap of believing that just because you’re in the cloud, you are automatically secure.

In order to identify your responsibilities, you should examine your Shared Responsibility Model from your Cloud Service Provider. Depending on the delivery model you may have full or partial responsibility for areas such as information and data, end-user devices, accounts and identities, applications, operating systems, network controls and so on.


System.out.println ("in method falseSwap
public class PrimitiveParameters

Conclusion

In summary, although it’s not always easy to determine and implement an ideal cybersecurity posture in today’s world, knowing the right steps to take – and the pitfalls to watch out for – will put you ahead.

Although cybersecurity threats are constantly evolving, many of the process and procedures to protect against them stay the same. With the right planning and a critical eye to seek out commonly overlooked issues, your business will be in an ideal place to mitigate risk.

WatServ

WatServ is an IT solutions provider that helps clients digitally transform their business through cloud technologies and services. Founded in 2006, WatServ specializes in providing hybrid and multi-cloud solutions and hosting complex, high-availability environments for enterprise-level applications. WatServ’s unique approach to planning, migrating and managing multi-cloud environments, plus premium 24x7x365 support, enables its global customers to focus on their core business. Relying on Microsoft and Google’s public clouds, in addition to its own private cloud, the company offers an ideal managed cloud environment engineered for security, reliability and performance. With offices in Canada and the United States, and with 1000’s of users connecting from around the world, WatServ is always on.

For more information, visit www.watserv.com