TIP Publication Date
July 14, 2015

Cybersecurity Building Blocks

Start with these Five Fundamentals

Data breaches and other Cybersecurity events are appearing in the news more frequently, and at this point the message should be loud and clear: it isn't a question of "if" you get breached, but rather "when" you get breached, what will you do next? In fact, the "when" could quite possibly be right now, and you don't even know it. An alarming metric is that it takes an average of 240 days to detect a breach, and the vast majority of these detections are from sources outside of your organization (FBI, local law enforcement, your vendor partners, clients!).

As we shift our attention from the news story of the day and the sigh of relief that it hasn't happened to us (yet!), there is great temptation to bring in vendors and/or load up with the latest appliances, technologies, and tools to keep your company and client data safe. It is very easy to get caught up in an arms race of sorts, stockpiling defense mechanisms and talent without fully thinking through the holistic implication of such action. Next-generation firewalls, security appliances, cloud-based mitigation services, infrastructure upgrades, and a mounting pool of new detection tools can be confusing and disruptive to the task at hand.

However, adding new weapons to your Cybersecurity defenses can actually make you become *more* vulnerable (additional platforms to be patched, greater vendor diversity, and the learning curve to become expert with your new toys) so this Trexin Insight Paper encourages a pause to review the fundamentals before moving ahead to other elements of your defense in-depth implementation.

Tying back to previous Trexin Insight Papers, we always evaluate current and future state goals against People, Process, and Technology, and your security posture is no different. The five fundamentals we will discuss are:

1. Organizational Roles and Responsibilities
2. Determine Toolset/Technology
3. Processes to tie the people with the tools
4. Sanitize your environment
5. Create a baseline

Fundamental Component #1: Organizational Roles and Responsibilities

The cornerstone of your Cybersecurity posture is the organizational design of the team that is ultimately accountable and responsible for its defense. It may sound simple, but your security team should have a clear understanding of who does what, who is an alternate/backup, and who to escalate to if ambiguities arise. Something as simple as not knowing explicitly who is expected to patch a given security appliance can create a significant vulnerability. A Risk role may or may not be in your security organization, and you need to determine that as well. If you do not have someone responsible for risk, I can assure you that it will fall to Security when you least expect it to.

WHERE SHOULD THE CISO REPORT?

In reality, where the CISO reports is as varied as the areas they are charged to protect, even within the same industry.

Despite the pros and cons of each scenario, the CISO needs ties to IT, GRC, Finance, and HR along with key business areas of his/her specific organization in order to stay plugged in to the spectrum of entities that control and determine how data is used.

While 50% of CISO's report to the CIO (according to Gartner), the remaining 50% report to a wide variety of executives: COO, CFO, CRO (Chief Risk Officer), CEO, even the Board. Whatever your company chooses, a dotted line approach can be very effective in establishing authoritative reach while broadening security and risk related discussions with non-traditional stakeholders.

You can group competencies (firewalls and switches may belong to Joe, while server and workstation patches belong to Kim) to maximize resource efficiency. Where possible, you should list a primary and a backup to ensure full coverage during planned and unplanned resource absences. You may want to leverage third party vendors to provide coverage if you have a small team or if you'd like to inject instant expertise to more rapidly increase your teams' capabilities.

In concert with documenting responsibilities, take time to establish career and training plans to help your team keep their knowledge current and relevant. While security-minded individuals are naturally curious and explore things on their own, someone needs to make sure resources are building knowledge relevant to the current and strategic direction of the company.

With your team design set, you may now move forward and make sure you have the appropriate tools in place. (Keep in mind, you may need to circle back to roles and responsibilities if you add, subtract, or change a tool.)

Fundamental Component #2: Determine Toolset/Technology

New tools and appliances are the candy that all techies long to unwrap and take for a spin! Given this temptation, it is important to be mindful of what you are putting into your environment for several reasons. A new tool or device represents another attack vector that you are exposing to the bad guys. Software and hardware tools each come with their own set of update frequencies, methods, criticality, and general overhead. In addition to yet one more thing to monitor and manage, you need to learn how the tool/device can work for you and make sure you are using it correctly. Especially in the security world, just about everything comes with logs and alerts that must be groomed and processed by someone or something—think SEIM (Security Event and Incident Management). Incorrectly using a tool can be just as egregious as not using it at all so make sure to validate and document each tool in your arsenal of defenses.

You should methodically and carefully evaluate each tool you own and compare its functionality with your business needs, along with determining who will own and manage it. Not to be understated, a completely viable solution is to use one or more external providers to absorb some of the workload — for example, you may not have an ArcSight (a SEIM product from HP) expert on staff, but you can contract with HP or a variety of other vendors if ArcSight is the tool that best meets your needs. The vendor can take responsibility for system maintenance, alert monitoring, event escalation, and tuning over time.

Chances are that you will find new things to do with existing tools, tools you thought you would no longer need, and the discovery of a new tool that fills a void. Make sure you fully understand the features, functions, and maintenance needs of your tools.

Fundamental Component #3: Processes That Tie People to Tools

As we have just learned, having a stable of tools at your disposal isn't going to make you any safer if you don't understand what the tools do and who is responsible for keeping them running smoothly. Now that you have an org chart telling you who does what, you've pruned your toolset to a lean, manageable catalog, and you've even groomed the alerts to be more meaningful, you need someone to look at those alerts and act upon them in triage manner: Is the alert real? What is the exposure level? What is the criticality? Who should be notified? Who fixes it, and what is the SLA expectation?

This component is where you review, revise, and/or create processes that document how your team should respond to a given event. While this should be a trivial exercise in constructing run-books for your tools, don't be surprised if you find yourself back at previous steps of identifying the people and technologies used in your defense systems.

One often overlooked truth is that security is the responsibility of everyone in the organization, not just the security team. Interestingly, security's role is actually to establish, measure, and monitor adherence and compliance across the organization. For example, the server infrastructure team may be responsible for monthly server patches and the security team may not even have the rights to install patches. The responsibility of security is to determine patch criticality criteria (e.g., "Critical" severity items must be installed within three business days and "Low" items may be evaluated and discounted for relevance/functionality) and measure that process guidelines have been met. To close the loop on this example, security should audit servers three days after the release of a critical patch to determine whether all servers were patched in accordance with the policy and to determine the disposition of any server that has not been patched.

Fundamental Component #4: Sanitize Your Environment

Now you have your People, Processes, and Technology completely thought through and documented. Nicely done! It's time to test all three components in a real-word exercise of interrogating the environment and making sure there is nothing malicious out there. As previously discussed, chances are very high that there is currently some form of undesired access to your data or systems occurring as you read this. You should prioritize a detection and remediation effort to occur as soon as possible. You are likely to discover that there is some further tuning needed to your org structure, your toolset, alert thresholds, and/or processes as you go through the sanitization exercise. Believe it or not, you are significantly maturing your foundation by iteratively working through these items.

It will not be quick, and it will not be easy, but taking a deep look into your internal and external networks will help uncover existing issues that you do not want to find out about from someone else. Reminder: you can expedite this and other activities by leveraging third party vendors to lead or assist.

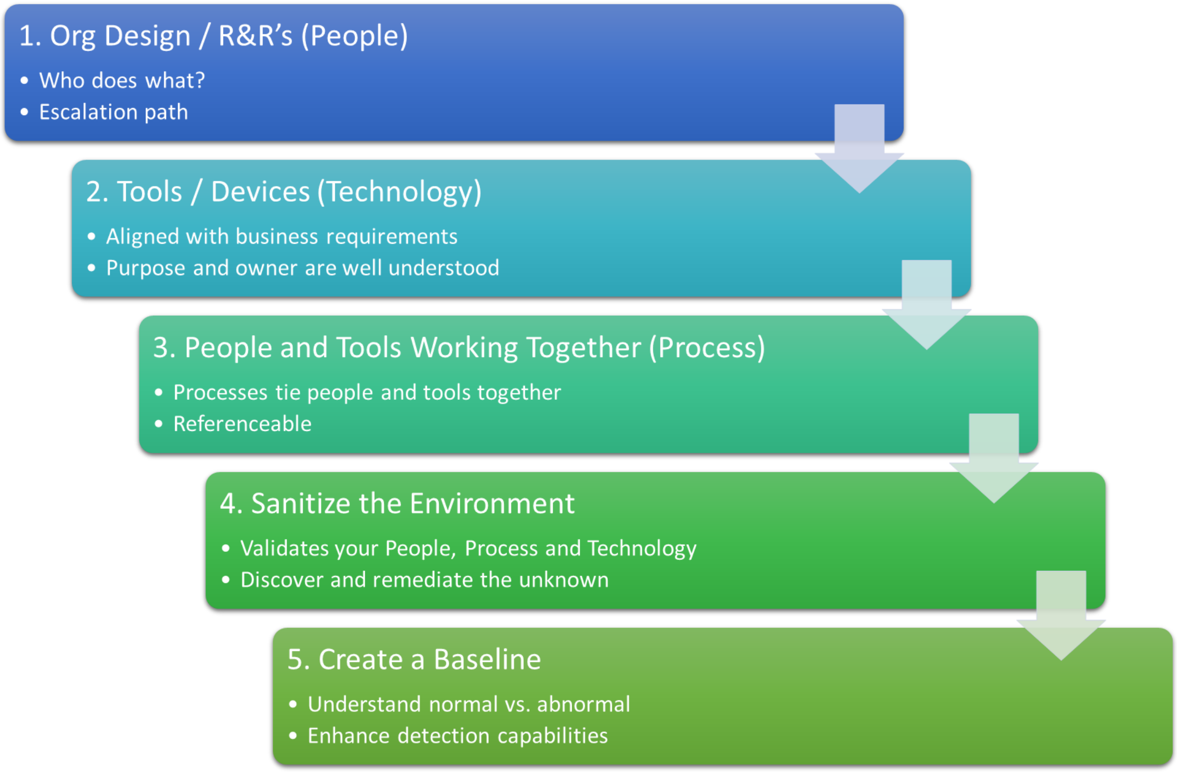
Fundamental Component #5: Create a Baseline

Building from the previous four items, you now have clear roles, a fully exercised toolset, and peace of mind that most of your risk elements have been addressed. The last component to our list of the five fundamentals is to create a baseline of normal computing activity in order to create a reference for when abnormal behavior is occurring. A classic example of what this means is as follows:

Over the past year, Sally has logged into the same six Finance servers between the hours of 8am and 5pm most weekdays. Suddenly, Sally's account is logging into HR servers during off-peak hours and creating zip files that are being stored locally. Without a baseline, we would not have visibility that Sally's credentials may have been compromised and are being used to log into other systems and assemble data for exfiltration.

Worth noting is that traditional anti-virus and anti-malware products work against signatures that compare running code against known patterns that indicate that something bad is happening. We are in a new age where known patterns are no longer the channel of choice for the bad guys. The detection landscape is evolving to rely on historical data and correlation of multiple, seemingly unrelated, occurrences in order to determine if malicious activity is taking place. Big data and forensic analysis are emerging as viable tools for mature organizations, but without a solid set of fundamentals those concepts represent more “noise,” distracting from effectively detecting and remediating unauthorized access to your network and data.

It is critical to understand your user and system behavior during normal operations so you are prepared when something abnormal is taking place.



1. Org Design / R&R’s (People)
- Who does what?
- Escalation path

2. Tools / Devices (Technology)
- Aligned with business requirements
- Purpose and owner are well understood

3. People and Tools Working Together (Process)
- Processes tie people and tools together
- Referenceable

4. Sanitize the Environment
- Validates your People, Process and Technology
- Discover and remediate the unknown

5. Create a Baseline
- Understand normal vs. abnormal
- Enhance detection capabilities

Conclusion

There are so many areas of concern to work through in the context of security and risk that it can seem insurmountable. Before moving into the heavy lifting (e.g. replacing your firewalls, installing new appliances, or conducting an Active Directory group membership cleanup) visit (and revisit) the foundational items we have discussed and make sure you and your organization are on solid footing.

> *BONUS ITEM – If you are feeling energized and motivated at this point, you could start right now with an evaluation of your vulnerabilities and risks to determine your tolerance and response plan for each. The outcome of this effort should be a prioritized list of agreed upon items that your company can turn into projects for proper completion tracking.*

Trexin Consulting experts have walked in your shoes and have helped organizations create stable and effective security foundations. As with any championship team, mastering the fundamentals is an absolute requirement before more advanced goals may be attempted and accomplished.

We can help, call us today.

This TIP was written by Ralph Carlone, who specializes in cybersecurity, program and project management, business process management and systems management. Ralph welcomes comments and discussion on this topic and can be reached at ralph.carlone@trexin.com