www.cybersecuritycohort.com

Cyber Security Cohort Podcast hosted by Heather Holliday

Episode 008 | Are You the One in Control?

In today's episode we'll discuss the importance of Controls and how Controls are used to ensure safe cyber practices. As Janet Jackson said, "It's all about control, and I've got lots of it."

I really can't even say the word "Control" without halfway singing it…at least in my head. I'm probably giving away clues to exactly how OLD I am when I tell you that Janet Jackson and I were pretty much in the same life stage when her song, "Control" came out.

It's true that as you enter adulthood you learn how important controls are. As individuals (and as companies) we want control because it's empowering. It means that you are making the decisions and taking the actions that *you* think are most beneficial. Without control, someone else is in the driver's seat, and they are going to take you wherever *they* want to go.

Companies rely on cyber security practices to help them keep control of their networks, systems, websites, and data. Policies and procedures also provide guidance to the humans involved in the business so that the company can continue to be in charge of its own destiny. After all, poor controls can lead to poor choices by employees that open the company to social engineering attacks. Poor controls by a company's vendors opens the company to attacks through their supply chain.

Here's where we can use a few of the important points Janet Jackson made about Controls to inform our cyber security practices. As she said, "Let me take you by the hand and lead you on this dance."

Firstly, are you in Control?

Every good Controls conversation starts with a careful and honest assessment of the control environment. You'll need to understand where you are most vulnerable. You'll also want to evaluate what types of practices put you at the greatest risk - whether that's the risk of the highest fines for non-compliance or actions that will ruin your company's reputation and send your customers running for the exits.

You have to know where you have confirmed gaps, potential vulnerabilities and where you are most secure. Knowing the state of the systems, websites, and even policies can help you make more informed decisions about the Controls you need to prioritize and where your time and money is best spent.

Even a fortress with a deep moat of swimming alligators has a vulnerability or two. Much like that fortress, often the biggest vulnerability is the human that is guarding the gate charged with determining who is allowed entry and who is denied.

Commonly, Impact Assessments and Risk Analysis activities are used to help you determine where you are in control and where your controls are most lacking.

One simple way to determine if you are in control is to simply ask yourself, (as Janet noted) “Can you make your own decisions?” If YOU aren’t the one deciding where customers are being directed online, you are clearly not the one in control.

So, how do you use Controls to get what you want?

Well, there are actually several different categories, or types, of controls. It’s important to understand what each type of control is and how it can be used to safeguard your company. If you are prepping for the Security+ exam from CompTIA, you’ll need to know these terms and be able to recognize the types of controls aligned to various scenarios.

The three biggest functional areas of controls include: Managerial, Operational and Technical controls.

#1 - Managerial Controls are the controls that are put in place by administrative actions, such as policies and procedures. The assessments I mentioned earlier (Risk Assessments and Impact Assessment) are a couple of actions that are taken under the managerial controls umbrella. Determining where you are vulnerable and to what extent is a very important practice in managerial controls. Many times these controls are intended to prevent human error or to deter internal threats from emerging.

#2 - Operational Controls are the processes that are put into place to ensure safe practices. This could include such things as your training programs on cyber security, the process of how security footage is reviewed, how guard scheduling is completed, or even the processes that you have in place to store and recover data. For example, using the 3-2-1 storage method can help. What is this method you ask? 3-2-1 stand for:

3 copies of the file
2 different types of storage options
1 copy of the file stored off-site

Like the 3-2-1 storage method, operational controls are intended to prevent ineffective or inefficient processes from becoming a security risk. Many operational controls require human intervention in order to be effective.

#3 - Technical Controls are the technological capabilities used to reduce risk or eliminate vulnerabilities. Everything from your encryption solution, to anti-malware software, to scanning software are included in this functional area.

Technical controls are sometimes called “automated controls” because they are intended to take the place of human action in order to mitigate risk. Technical tools, from formulas, to code scans and even full-blown applications help to mitigate the risks in both systems and risks that may be propagated by human behavior.

But, this isn’t the only way to think about the controls environment. It’s also important to consider where in the process, or at what stage of the game, the controls are used. Is it before disaster strikes or after the storm takes the roof off your house?

Preventative Controls prevent a problem before it happens. This works much like locking the front door of your house before you leave to prevent someone from just waltzing in and taking your stuff.

In the world of cyber security, preventative controls include such things as using a firewall, closing ports that don't need to be open, and using a virtual private network to connect to the internet. There are a whole host of tools, both hardware and software, that are specially designed to help prevent cyber security breaches.

Like your locked door, preventative controls may not always be clearly visible "on the surface" but when someone attempts to turn the doorknob, they'll quickly learn that it's not going to be as easy as walking through the front door. That doesn't mean they won't try that first, though!

Deterrent Controls, in contrast, are often intended to be clearly visible in order to deter bad actors. This includes devices like clearly visible security cameras, muscular bouncers at the front door of your club, or pop-up notices that tell would-be hackers, "Nope. Not today." If your company has a firewall that prevents employees from visiting well, more personal websites, a simple pop-up message of "You are not allowed access to this site," may be enough to deter them from trying THAT a second time.

Detective Controls are typically in the thick of the action. They are monitoring systems that are put into place to find when behavior doesn't fit a typical pattern, when an agreed threshold is breached, such as when an activity occurs with too great a frequency, or the activity is too infrequent. Surveillance cameras and log monitoring both fall into this category. Detective controls are looking for that "guy in a winter coat in July in Florida" or that IP address that has tried 19 times to access the site with the wrong password. The detective controls will alert you to the possibility that something could be wrong. Of course, there are no guarantees because maybe there wasn't a problem…just an unusual occurrence.

In the case of detective controls, there is often a mathematical formula that is applied to determine the upper and lower bounds of a threshold, such as using a mean (or average) to determine what would be a reasonable, or standard deviation, from the norm. So, if you thought that statistics class you were required to take wasn't going to be useful, well, this is where you learn the value it can bring…even in cyber security!

Compensating Controls are usually trying to compensate for, or make up for, a primary control that is either known to have failures in certain circumstances or is used to control something that is simply too important to leave to one control alone. Consider our locked door again. The locked door may be the primary method we rely on to keep people from walking into our house, but maybe you also have a big, barking dog that would also effectively stop just anyone from walking in. The dog, in this scenario, is your compensating control. It's helpful just in case you forgot to lock the front door.

In a cyber security context, you may have a technical control that you rely on, such as a badge scanner, to keep only employees from entering your place of business. If their card somehow becomes defective, or your badge scanner goes down for any reason, you probably want to have another way to guarantee that you know who is coming and going from the building. Compensating controls, like a sign-in sheet and a guard checking IDs at the front desk can be used as compensating controls.

There are, in fact, even more ways to talk about controls than those that I mentioned. If you do an internet search, you can probably come up with another half dozen control types or labels. Other common terms you can explore include "physical controls," "human controls," "corrective controls," "response controls," and more!

Are your Controls all grown up?

Well, that's actually an important question. You'll want to continuously review and analyze the effectiveness of your controls to see if there are any changes that are needed. Changes in technology, for instance, often drive new opportunities to replace "manual controls" with more "automated" options. There are other factors, too. Changes in legal requirements, the political landscape and cultural shifts in risk tolerance are all factors that can drive changes to your Controls practices.

Janet also asked, "When are you going to stop?"
Her answer was 100% right. **Never.** If you want to maintain a cyber safe company, you'll need to continuously monitor, evaluate and make changes. I'm sure that the person who first invented the deadbolt lock would never have imagined all the tools we now use to keep our homes safe.

Similarly, there are technological changes happening every day that will both enable safer cyber security practices AND add new challenges. Keeping up with current trends and always being willing to make adjustments to your controls is an essential practice in cyber security.

Finally, I'll just add…Janet is SO correct. "So make your life a little easier. When you get the chance just take Control!"

Thank you for joining this episode of the Cyber security Cohort. This is your host, Heather Holliday. Join us next time for another step in our journey of 1000 miles toward cyber security expertise.

Episode Notes & References
Information shared in this episode came from personal experience. More information on these topics can be found by searching these references.

- Janet Jackson's "Control" video: https://www.youtube.com/watch?v=LH8xbDGv7oY
- 3-2-1 Storage Method: https://youtube.com/shorts/FbMdH3d00l0
- 3-2-1 Storage Method: https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf
- CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson: https://www.amazon.com/CompTIA-Security-Get-Certified-Ahead/dp/B096D1LGSK