GEISEL SOFTWARE

BUILDING A CULTURE OF SECURITY

How to Meet Standards of Security
Without Making Your Team Hate You

TABLE OF CONTENTS

Building a Culture of Security

By Liz Couture, Geisel Software

You can't turn on your television or surf the Internet today without hearing about some sort of data breach or security attack. Our homes, workplaces, and products have become increasingly interconnected, and cybersecurity has taken center stage as ransomware attacks on school systems, medical devices hacks and the latest password hijacks have become daily news. And with the shift to remote working this year, many companies have experienced increased security issues.

But how do you implement security practices? You may be tempted to go down a list of security do's and don'ts and commit to implementing every single suggestion. And if you need to comply with a standard like NIST 800-171, purchasing a large, one-size-fits-all security software solution and changing all your policies to immediately meet all standards MAY look like the way to go.

But you'll often find that companies that do those sorts of things end up having networks and policies that sound very secure on paper but aren't actually very secure at all. They have passwords that change every week, so everybody writes their password on a sticky note on their monitor. They have hugely secure networks that don't work well with automated builds, so everybody does all their work on the guest WiFi. They have policies that are impossible to comply with fully, so employees stop even trying. Instead of trying to implement every "best, most secure" policy — especially when your resources are limited — you should create an environment where all employees value and are invested in security. You need to build a culture of security.

Start by defining your security needs.

Often, especially for a small business that is just beginning to consider cybersecurity, security needs are derived from an arbitrary list found on the Internet. But employees don't care about a list; they care about doing a good job, making a good product, and not being the one responsible for your company getting hacked. To get buy-in from everybody on your team, your security policies need to be rooted in the actual needs of your company. So how can you determine what those needs are? Start with listing the vectors of attack that your business is likely to face. If your office has a lot of temporary workers, high turnover, or clients using your machines, you should probably be concerned about physical security. In that situation, it makes sense to keep confidential documents out of sight and to sign people in or out of areas with potentially valuable information. But if your company consists of three engineers working out of your garage, it's highly unlikely that a stranger is going to walk in and stick a USB drive in your computer without somebody noticing. Likewise, if each of your employees is developing and hosting several web applications as part of their daily work, your exposure to outside hackers is very high, and you need stringent network

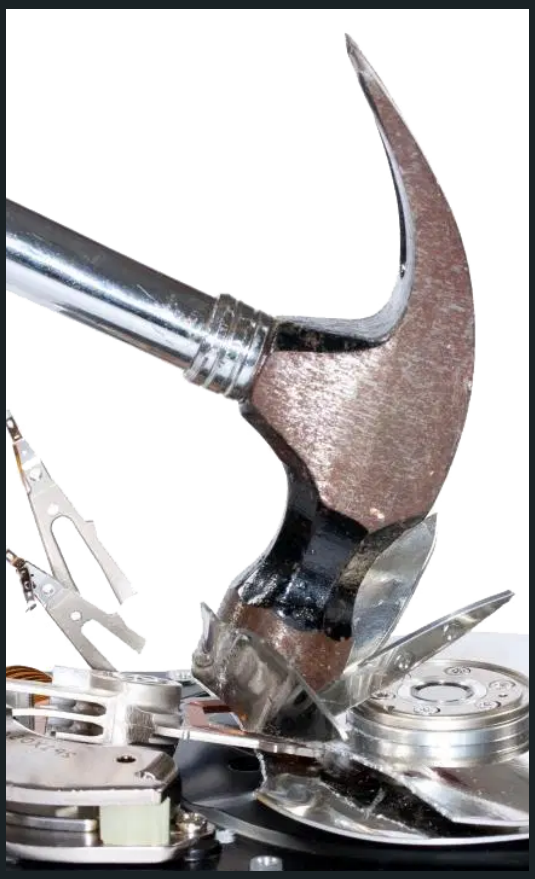
security. But if you just have just one static website representing your whole company and there aren't very many places that your network is exposed to the outside Internet, that might be a less vital part of your security plan. When you determine what your danger areas are, you can create a security plan that addresses and defends against those risk factors. This approach helps your employees understand why they're being asked to implement certain processes that help address your security risks.

"Walls don't just keep hackers out. They can also keep your employees from doing their jobs effectively."

Layer your security.

Often people think security is just building a huge impenetrable wall around your company to keep the bad guys from getting in. But walls don't just keep hackers out. They can also keep your employees from doing their jobs effectively. Think about it. We don't surround our houses with huge, impenetrable walls. I have a fence around my backyard, but anybody could get in just by flicking the latch. That just gets them into my back yard. I still lock the back door of my house and arm my security system. And even if someone was able to get past all those checkpoints, my most important documents are locked in a safe in my basement.

We should be building our network security the same way. Known low-risk areas of your business should be more open and useable, and the high-value and high-risk parts should be well secured, even if it's more difficult to comply with those security practices. For example, if your company deals with any Controlled Unclassified Information (CUI) that is accessed on a portable device — whether that be a laptop or a mobile phone — you need to implement a series of controls. That may include criteria like the device must be under the control of your business, you must manage when portable media like USB devices are used on it, it needs multi-factor authentication at all times, it needs to time out after a certain period, and more. If you tried to implement those policies throughout your entire office network, it would significantly impact all of your remote employees. They would either need to stop working remotely or give the company considerable control over their own personal devices, even if they weren't working on the CUI project. If only some of your projects involve working with CUI, it's a better idea to create a separate internal network just for those projects and documents.



Put it on a computer behind a locked door with all the security features required to work with that kind of data and let your employees who aren't dealing with projects of that same level of risk continue to do their work unencumbered.

Never make a security policy you can't reasonably expect your employees to follow.

Once, at a previous job, I attended an employee assembly to discuss the company's new security procedures. Some of the new changes were reasonable, like limiting employee access to patient data to times that it's truly necessary because the company would now be logging all interactions employees have with patient data. Other policies sounded fine on the surface but were, in practice, very difficult to follow. Specifically, they were ending a policy of allowing employees to take home old computers after they were no longer in use. In addition, any computer that was ever used to access patient data but was no longer used for work needed to be returned to the company or the hard drive needed to be physically destroyed. I raised my hand and asked "Once, while I was providing on-call support last year, I had to access patient data on my ex-boyfriend's computer. Does that mean I have to track him down and smash his hard drive with a hammer?" The presenter thought about it, replied "Yes" and moved on with the presentation.

Theoretically, I can understand the policy. The company didn't really believe that my failure to smash a hard drive that temporarily accessed patient data years ago could ever actually result in a hacker obtaining patient data. But as a manufacturer of medical devices, they needed to comply with certain security regulations they had agreed on and implementing the "smashed hard drive" policy allowed them to check off that box. And in the extremely unlikely event that it ever became an issue, they could blame a failure to comply with that policy on me.

What this company didn't consider is that implementing that policy in the first place resulted in their employees thinking they didn't take security very seriously. Employees presumed they weren't really expected to comply with the security policy because no one could comply and expect to get their job done. This led to employees slacking off on complying with their other security policies as well. They didn't worry about sending things from their personal email or holding the door open for people coming through the badge access door behind them because their perception was the company wasn't actually serious about security.

Don't pit security against effectiveness. You'll lose.

If you find that your employees aren't complying with your security policies, you shouldn't assume they don't care about security. What may be happening is they are more focused on getting their job done and perhaps don't have a good understanding of why your security policies are needed to protect against specific threats. Or maybe your policies have been implemented in a way that makes it difficult for your employees to do their jobs.

For instance, most engineers need to regularly install software on their computers to work on their projects. If your policy is that engineers can only install software on their computer after it's been approved by a designated person and that process is cumbersome and begins to interfere with their work, they'll just stop telling you when they install new software — unless they understand why it's important to the company to have such a stringent policy.

At Blackhat this year, Dino Dai Zovi compared cybersecurity to designing a better parachute (you absolutely need to watch his keynote address https://www.youtube.com/watch?v=8armE3Wz0jk). He explained that you can't just tell your software engineers to stop jumping out of planes; you need to build your security systems around making it safe for them to do so. My takeaway? Only by understanding your employees' network requirements can you start to make policies that both enable employee productivity and keep your company safe.

Test your employees.

Developing a culture of security doesn't happen overnight. It's an ongoing process. When I worked as a lifeguard at Six Flags, my bosses didn't just escort me to my lifeguard chair and disappear. They would regularly toss a plastic baby doll into the water I was guarding and count the seconds until I rescued it. They'd fake choking in the lazy river and pretend that a stuffed carnival toy lying in the grass needed CPR. At first, this was stressful, but eventually being highly attentive became second nature and responding to those lifesaving events became less stressful.

Similarly, if your employees are getting an email that looks like a Phishing attack every other week, they're going to get much better at recognizing

"Telling people to follow security policies is nowhere near as effective as training them using real examples of the threats your company might encounter."

and appropriately responding to an actual Phishing attack. Drop some USB keys in the hallway that contain nothing but a file called “DON’T PUT STRANGE OBJECTS IN YOUR COMPUTER.txt”. Try to hack your own website. Telling people to follow security policies is nowhere near as effective as training them using real examples of the threats your company may encounter.

Take shame out of the equation.

There is an important caveat regarding testing your employees: it needs to be done in a way that doesn’t put people on the defensive. If you shame people for making a mistake, it will prevent them from reporting future mistakes. It will also drive a huge wedge between your security team and the rest of your employees.

The fact is, everyone makes mistakes. The surface for attack is growing exponentially as the world becomes more connected and security is more complicated than it’s ever been. It's hard to keep up with the hundreds of constantly changing "best practices," so it's not surprising that mistakes get made. And a large part of security is analyzing mistakes made, fixing and documenting the incidents after they've occurred, and enhancing our systems so they don't happen again. Responding to mistakes with a “Whoops! Thanks for telling me.” attitude instead of saying “I can’t believe you fell for that!” will go a long way towards making employees feel comfortable reporting any potential issues. The result is a team that works together to continually improve your security.

Don’t get caught up in the hype.

It’s easy to get caught up in all the security hype, and before you know it you convince yourself you need to immediately implement every suggested security standard. But don't cripple your company with unnecessary policies. Security IS a very real issue and you do need to develop a set of standards for your employees to follow, but it’s important to evaluate your specific vulnerabilities and develop procedures to address those issues while still allowing your employees to work in a productive and effective way. When you have security policies that make sense, you'll develop a strong culture of security where employees are invested in keeping your company safe.

About the author: *Liz Couture blends user needs with regulatory compliance requirements to develop effective software applications. Her experience spans from enterprise software architecture design to interactive mobile apps. At Geisel Software, she develops software solutions for the medical device and robotics industries with a focus on security, reliability, and ease-of-use. She is a Clark University graduate.*