Building Better Cybersecurity in Your Organization

By John Tooley

Each year, the number of data-breach victims is higher than the last. This means that U.S. organizations – corporations, non-profits, institutions and governments – collectively begin each new year knowing it could be the worst year ever.

Despite all the attention on cybersecurity, there is no turnkey solution that eradicates the threat. However, companies can help shield themselves by building awareness and a strong sense of community.

Today, as businesses become more digitized – with an increased demand to provide a safe and secure digital framework – it is important to recognize that cybersecurity is no longer merely an Information Technology problem … it is a business problem. According to a recent Forbes article, "If recent global security breaches impacting over 200,000 computers in 150 countries and costing millions are anything to go by, it could not be clearer that cyber security impacts businesses as a whole, not just IT departments."

Security requires a community. It isn't something that can be assured by a single person on his or her own. And because it's a foundational need, people have evolved to possess an instinct to help create safety and security.

At Cast & Crew, one of our core values is security – so it's no surprise we take security awareness seriously. Recent security-breach incidents around the world have heightened our vigilance and underlined the importance of taking even stronger measures to protect both our employee and client data. Cast & Crew handles highly sensitive and confidential information daily. As such, it is of utmost importance – and our duty – to take the necessary actions to implement, follow and equip our employees with comprehensive security tools.

There is an unofficial motto in cybersecurity: "People are the weakest link." The motto was adopted because it's true – you can trace almost every hack back to human error. Think about it: A person didn't configure a website correctly, fell for a social engineering scam and gave away the password, or didn't build secure code into the software. People are often at the root of the problem … but they are also the solution.

Rather than seeing the people in an organization as the weakest links, we believe the stronger solution is to empower employees to be "human firewalls." We all have a role to play. Security is everyone's job.

Without security, you can't evolve from meeting basic needs to functioning as a society. This is why security is everyone's job. Just like our physiological needs, security is a building block to our own personal fulfillment. And this is why we need to let everyone have a chance to play a role in protecting that. We all have a stake in the results.

So how might we give everyone a chance to participate? DEPUTIZE THEM!

What does deputizing people for better cybersecurity look like? It means both giving them something to do and giving them the authority to do it. This can be incredibly empowering for the deputy. It means each and every person is important and valuable – and it strengthens the entire organization as this empowerment spreads to more and more people.

This sort of effort obviously entails more than just putting up posters around an office or organization with things like “See something, say something” written on them. We believe there is more to it than that and have outlined a quick checklist of best practices an organization can follow:

6 Steps to Creating a Cybersecurity Program:

1. Provide a **method for people to report potential security issues.** This could include suspicious emails or activity. It could also mean offering suggestions to help improve their business practices, like not sending sensitive information via email.
2. Create a **security council** and make that a real part of security governance. Let the members of that team help prioritize the risks to manage.
3. Craft **cybersecurity newsletters** to share real stories about how cybercriminals have affected business. Putting a face on the issue helps create a human connection to security. Focus on your industry to create familiarity.
4. Regularly conduct **incident response drills** to help employees become more aware of recommended procedures. Assign departmental leaders or deputies just like in a fire drill to help organize and report on progress.
5. Create an **awards program** for employees that reward their contributions in protecting cybersecurity.
6. Recognize vigilance. Give credit to people for being a part of reporting or helping respond to an incident. Have a **shout-out email list**, or a newsletter with their pictures.

Incentivizing good behavior is important, but creating a culture that moves beyond incentives and gives employees purpose is what will make the biggest difference in our cybersecurity program.

Cast & Crew’s values are Quality, Integrity and Security. They also are the foundation that supports our cybersecurity program.

John Tooley is the VP, Senior Security Information Officer at Cast & Crew, where he designs and builds optimized security, risk and compliance programs. John has nearly 20 years of experience in the entertainment information technology security sector.