Best practices Security operations

6 min read

How to build stronger security teams

By Brooke Lynn Weenig, Senior Product Marketing Manager
Jayson Street, Chief Chaos Officer, Truesec

July 25, 2023

Security management

The security community is continuously changing, growing, and learning from each other to better position the world against cyberthreats. In the latest post of our Community Voices blog series, Microsoft Security Senior Product Marketing Manager Brooke Lynn Weenig talks with Truesec Chief Chaos Officer Jayson Street, who wrote "Dissecting the Hack: the f0rb1dd3n Network" series and featured on the National Geographic series "Breakthrough Cyber-Terror." The thoughts below reflect Jayson's views, not the views of Jayson's employer or Microsoft, and are not legal advice. In this blog post, Jayson talks about security awareness training.

Brooke: Tell us about yourself, Jason.

Jayson: I have always found that it was better to make bad guys have bad days than to be a bad guy. I used to work defending banks, and I was so good at that, I started testing their security. Through doing that, I realized I was good at robbing banks, and so now, I virtually "rob" banks for a living to help people be better protected and secured. I rob banks in Jordan and Jamaica and from Lebanon to Louisiana. I have robbed hotels from Malaysia to Germany to Maine.

I make sure that I get caught because I am not there trying to break things. It is about education, not exploitation. I am there to teach, not to test you. I go back after I have compromised the site and educate every person who let me do something that was bad. I tell them, "I lied to you. I was doing a bad guy thing, and this is what you can do better. Now you know what it looks like." I turn this negative experience for them into a positive one.

I do not record the names of anyone who fails that part of the test. I record the people who did something good because then you have someone for employees to look up to. No matter how bad the report is, people can say, "Bob in accounting questioned the attempt. He did the right thing." I have had to do some of the most outlandish things to get caught but I guarantee that I will get caught by the end of the engagement.

Brooke: How can organizations and people improve their security posture?

Jayson: People say, "We are different here." No, you are not. People are people. The myth that a person is built differently or runs internally differently is absurd. When anyone is at a workspace, you have certain expectations versus the expectations if you were in a public place. Your mannerisms change from the workspace to the public environment.

I gave a talk last year where I talked about perception. If I dress up in a suit, have a USB drive, and am coming in to do an audit, I am going into a private area. I have already made it through your first layer of security because that is usually a joke. One time, I walked straight to a bank's breakroom, sat down, drank some water, walked into the teller area, did not even say anything to anyone, just nodded to the guy depositing money beside me, unplugged the computer, and walked out of the bank with it.

Improving security posture, including training your employees well, is important. On the first day of your job, you were told what is expected for your job. They tell you what your role is going to be, and they show you what equipment you have, and that you are responsible for that equipment. If you were given a van, which is a piece of equipment, do they give you the keys on the first day without making sure you have proper training and understand all their rules? When you are given a laptop, it is a piece of equipment. You were told that you were responsible for not just how you operate this equipment but also the security of this equipment.

The first time you click on a phishing link, whether it is a test or not, no harm, no foul. But all you have to do is go through an extra hour of training. The second time, in order to train employees better, I suggest that you do something more along the lines of, "Your email has now been turned into a gateway. All your incoming emails are held on our server, and we send you a whitelisted digest. You must go through the emails and check the ones that you want to receive. You are going to have to do that for three months. If you click on a third phishing email within the same year, you are fired." Security must be top of mind for your employees to improve your security posture.

Brooke: **What are the current top threats you are seeing and have they changed?**

Jayson: The technology keeps improving and it is harder to break. We are stuck in the mindset that we still need to break technology or we can just buy another blinky box to combat people breaking into technology. The defenses are not going to be walls anymore. Walls don't work.

People need to protect technology instead of trying to make the technology be the barrier for the people. Technology should be the safety net for when people make a mistake because more attackers are no longer going after the technology. In our industry, we want things to be quick, but if you are not doing patch management and asset management, you are not going to be prepared for anything that is going to happen. They are the foundation.

People forget that foundations are demanding work. They are ugly. They are concrete blobs. There is nothing pretty about a foundation, but if you do not have one, it does not matter how pretty that house is that you are building on it. It is not going to last. We must work on our foundations and make sure when a new machine pops up, someone gets an alert saying the machine popped up on the network.

Brooke: What advice would you give to chief information security officers (CISOs) on security awareness training?

Jayson: It is okay to not understand all the different technologies. It is hard to combat the Hounds of the Baskerville syndrome, which is when Security comes to you and says, "We did a really excellent job this year. Nothing happened. If you give us $2 million more for next year's budget, we will make sure nothing happens again." If the hounds are not barking, how do you know how they would respond in a threatening situation?

To succeed at securing their enterprise, the chief executive officer (CEO), chief financial officer (CFO), and chief operating officer (COO) need to live by the security policies they establish. If the CEO is taking patch management seriously, if the CFO is making sure their badge is visible when they go into work, if the CISO is making sure that their workstation gets locked out after 15 minutes and turns onto a screen saver or lock screen, then the people who report to them know to take security seriously. And then the people who report to those people will do it.

If a CEO or a CISO says, "That does not really apply to me," every person beneath them is going to say, "I work for them, so that does not apply to me," and every person who works beneath them is going to say the same.

Tell the executives, "If you were breached for five minutes and a quick-thinking employee realized what happened and you can start your incident response within five minutes, that is going to cost you a week's worth of time to make sure everything is taken care of. Imagine how much time a breach is going to take if that lasted for five months."

Brooke: How should the cybersecurity team respond when an employee clicks on a phishing link?

Jayson: I have never met a server that got upset when they got popped with Microsoft 365. But when a person clicks on an email or makes a mistake and allows someone in or answers a phishing email, how we respond to them matters because they do have feelings. One of the biggest myths is when people say a "stupid user" clicked on a link or went to a website. I do not think people are stupid. I just think that information security did not properly train its users.

Cybersecurity should let people know that they are not a liability but an asset and part of their team. Employees have feelings and they do not want to fail. Many insiders are not an insider threat because of maliciousness. It is because of ignorance. But ignorance means that you can be educated on it and learn. And that is the most vital part when securing your organization.

Learn more

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility