CYBILITY

Demystifying Cybersecurity

Cybility Savvy Podcast

Transcript of Season 01 Episode 01 – Who would hack us?

Welcome to Cybility savvy, the show that demystify cybersecurity for not-for-profit boards and leaders. I'm your host Michala Liavaag Founder of Cybility consulting.

Today I'm going to shed some light on what cybersecurity is and why it's important for not-for-profit organisations.

Quite often I'll hear cybersecurity Why would we need cybersecurity? You know we're a not-for-profit organization, working for the good of society, who would actually want to hack us anyway? We're charity, we don't have lots of money and we might not be dealing with sensitive data, depending on the type of charity you are. There's lots of variations on these, and I've heard them so many times that I decided to actually let's start this podcast as another way to help you build customer trust and protect your organizations.

So back to basics. What is cybersecurity? Fundamentally, it's about the protection of devices, services, and interconnected networks, and obviously the information on that, and that's what we value from attack, whether it's like theft or damage by some sort of digital electronic means. Generally speaking, we think of it as being connected to the Internet.

There is a difference between information security and cyber security. Information security is wider than cyber security in that it's looking at information in all its forms, so that might include on paper a photograph in an album microfiche. Lots of other things other than just digital systems. Cyber security is very much focused on those digital systems, and as I mentioned earlier, typically connected to the Internet. So, think about all these smart gadgets and things.

So, coming back to the other question around why do hackers target charities? That's something that I get asked quite a bit. And it's not necessarily that they're actually targeting a charity, some do, and I'll give an example of one in a moment. But generally speaking, charities and other not for profit organizations end up as collateral damage because it's so easy with attackers on the Internet that they can send their attack out to people all over the world and just see what happens. See, who bites. The wannacry is a good example of how it wasn't really targeted at the NHS. But they were involved in the fallout, unfortunately.

The other thing I'd like to just cover off for you in terms of sort basics 101 is about the goals of cyber security, of information security. We have something called the CIA Triad, and that's referring to confidentiality, which I imagine most of you associate with the security anyway, about you know keeping things protected and to the only people who should have access to them. But also, there’s integrity. Now, this isn't about the integrity of the person, but integrity

(c) September 2021 Cybility Consulting Ltd, all rights reserved.

of the data. Is it accurate? Has it been changed by somebody who shouldn't have been able to change it? You know, think about say healthcare organizations where you might have infusion pumps and if something was changed there that could actually have a real physical harm impact on somebody.

Then the other big one is availability. Now, generally speaking, most people forget about this being part of security, but making sure that your systems are actually up and available at the time that you need them is absolutely fundamental part of security, and many of you, especially the large organizations will have your own IT departments who very much focus on the uptime of their systems.

So, what I think about the people who might attack an organization and let's just think for a moment about the people externally. What harm can they actually do to an organization? There's quite a few examples and I remember there was one where at the British Pregnancy advisory service. They were hacked by a 27-year-old who was anti-abortion. So, he is what we class as the hacktivist and unfortunately UM they were actually fined 200,000 pounds by the Information Commissioner's Office, because it was deemed that they hadn't protected the information well enough. Now it's a bit difficult because certainly as a charity you might also think, well, they're the victim here, but the rules are as they are, and in this case, the ICO felt that they could have done more.

So, think about it. Are you doing enough? What is enough? That's something we come onto in another podcast episode.

Then there's a nice example of, well not nice it's rather awful, actually. Some cybercriminals did actually target a charity, a Hospice up north, and they used a combination of attacks both phishing via email and then speaking on the phone, and they managed to steal 500,000 pounds from that charity. So, money is one of the huge motivators and when you work so hard to fundraise that money its particularly painful.

And then the other one. There are lots of different types of attacks, by the way, I'm just picking some out of here as examples. Nation states. So, everyone always talks about that there's this cyber war going on in the background and there is and certainly throughout the pandemic you'll probably have noticed on the news, some stories around Nation states trying to steal intellectual property from universities and big pharma, for example. So, there are lots of motivations for all this, and lots of reasons why not for profit organizations might get caught up in it and need to do something to protect their cybersecurity.

Now it's impossible to protect your organization 100%. Anyone who tells you they can is lying. Don't buy those products where they say you can. It's not true. What you can do is make yourself a harder target than the next organization. Now, smaller organizations actually have an advantage here because you probably have fewer systems, fewer people, and a lot less complexity than the larger organizations, which means it's easier for you to secure them.

(c) September 2021 Cybility Consulting Ltd, all rights reserved.

As a leader, I think the most important thing that you can do to protect your organization is to set that right tone from the top and lead by example. So, a couple of things that you might want to do; Be vocal about that vital role, that information that cyber security play in creating more resilient organizations. Praise your people when you catch them doing the right thing, whether it's clearing a desk or reporting a phishing email that manages to prevent an attack, for example.

Remind everyone that cybersecurity is a shared responsibility, and that's never more so important than in this post pandemic world where people working from home remotely and also that hybrid going in and out of the office, so you know if for those organizations that do have a security team.

The security team can't be there in people's homes. People need to be their own security teams. That's a really important thing that you can help promote that message.