Cybersecurity Best Practices

Businesses in every industry are facing cyber threats with increasing frequency and severity. It is no longer a question of *if* your organization will experience a cyber incident, but *when*. From employment/HR data breaches to operations disruptions to wire transfer fraud and more, today's landscape is brimming with real threats promising real and costly business impacts.

Earlier this month, our team in Nashville pulled together a group of industry experts for a panel discussion to discuss the current cybersecurity environment and best practices for businesses to prepare for and respond to potential incidents.

The following Q&A includes insights from our guest panelists, including:

Robb Harvey, Partner, Waller Law
Chris Morris, Partner and Senior Vice President, Benefits Communications Inc.
Darren Mott, Owner, Gold Shield Cybersecurity
Corey Ross, CISSP, IT & Information Security Professional, Checkpoint

What are the most common threats businesses face today?

1. *The FBI puts out a report ever year called the IC3 Cyber Crime Report. The number one threat every year is* ***business email compromise****. The methodology by which that works is varied, but it all comes down largely to social engineering. 90% of intrusions into a business' network is going to start with a human factor – someone click a link somewhere. The reason social engineering works is because someone always clicks a link.*
2. *From a threat perspective, business email compromise is number one from a financial perspective as far as general loss. Ransomware gets all the news, but* ***business email compromise creates 29x more loss per year than ransomware.***
3. – Darren Mott

How do you go about building defenses and implementing best practices?

1. *Once you understand why you should defend your networks, especially something like email, you put technology in place to negate the human factor – AI-based tools like anti-phishing or intrusion prevention. Technology has to help you. Anything you throw into your environment related to security is going to slow your production down. Security in essence slows you down, but if you marry the two together, it keeps your business running.*
2. – Corey Ross

1. *When you apply for insurance, the insurance company is going to give you a multi-page list of things that you have to have in order to get insurance. You have to have an incident response plan. It has to be adequate. It has to be looked at and tested by the insurance company. You have to have an outside lawyer assigned as your incident response or data breach or ransomware person. … Make sure that when you have an incident, your first call should be your outside lawyer. What that outside lawyer adds is the umbrella of the attorney-client privilege which you have to have. You need that privilege as soon as you have an incident.*
2. – Robb Harvey

What are some misconceptions about cyber risk?

1. *No one expects to be a victim, and no one thinks they have anything that anyone would want. Tell me what your business does, and I can tell you who would want your data and why they want it. There are always going to be the criminals who want it from a financial perspective. Data is valuable.*
2. – Darren Mott

How do you assess the potential impact of a cyber attack?

1. *The first step is to have a proper tabletop discussion with your business area owners, including finance and HR. You have to start with an honest discussion, "If Process A goes down, how long can your business survive?" The average I've seen lately is something like two weeks before a business has to shut its doors. And so, it's a matter of knowing where that point of failure is and what your maximum tolerable downtime can be. Once you understand those numbers, you can start to implement your technology around it to make sure you can get everything back up and operational should the worst case happen.*
2. – Corey Ross

What can a business do to minimize risk when selecting a benefits technology partner?

1. *As you pick an employee benefits provider from a benefit administration perspective, you are going to be sharing sensitive information with them. Make sure in their master services agreement that they have the right insurance limits based on the size of your organization. Also, make sure they have a SOC 2 certification or a HITRUST certification, ensuring that there is a third party that is going in and auditing their business practices, so you know they are managing your data on your behalf in a secure fashion.*
2. – Chris Morris

There are a lot of considerations when creating an incident response plan. What are the critical elements to an incident response plan?

1. *The key element to an incident response plan is to first have your playbooks built first. It can take a long time to get a solid incident response plan. Having a playbook that states, "This is what we need to do, step by step for ransomware or a rogue employee or whatever the incident may be." Having this in place is really going to help calm the chaos.*
2. – Corey Ross

1. *You can buy an incident response plan off the internet. I don't recommend it, but you can buy one. The reason it doesn't work is because there is no buy-in from anybody at the company, nobody really cares. So, you need to have a great plan that is designed for your company, probably brought to you by your outside forensic consultant. And then you have to really rehearse it and have buy in. …. You need to make sure you have your outside forensic consultant lined up for when you have a breach. You need to make sure you have your outside lawyer on call for when you have a breach.*
2. – Robb Harvey

Contact your Scott Risk Advisor or Benefits Consultant with any questions about your business' cyber risk and to ensure you are properly prepared and covered for potential incidents. Keep an eye out for an upcoming Risk Matters podcast featuring audio from this insightful panel discussion.