Cyber crisis: Out of the Shadow

[Description] With cyber threats constantly looming in the shadows of cyberspace, achieving readiness with the right tools, frameworks, and action plans is the key to bulletproofing your enterprise. Formulate your cyber crisis response and build a mitigation strategy in this podcast with Neha Sharma, MBCI, and ISO 22301 Lead Auditor.

Imagine that you're finishing up your day and preparing for that evening cup of coffee. But before you do, you hear a ding! And then another notification – a critical system has been taken down. Then follows a flood of emails, and you feel a surge of adrenaline. Soon, your Ops team is in chaos and everyone is wondering – what hit their systems in a split second? You resolve to NOT panic, and reiterate your cyber crisis response plan to your team – that is, if you have one in place.

Hello everyone, and thanks for dropping in! This is the cyber security podcast, and I'm Neha Sharma – MBCI and ISO 22301 Lead Auditor from HCL Technologies. And as you have probably already guessed, today we are looking at some of the challenges that organizations face when hit by a cyber-crisis, and how you – can better prepare for them with a cyber-crisis response strategy.

With so many businesses undertaking digital transformation initiatives and making the move to the cloud, cybersecurity concerns have kept growing, and with good reasons. Recently, we saw SonicWall state in its Cyber Threat Report that there were 5.4 billion malware attacks and 5.3 trillion attempts of intrusion over the last year. And that's not all – for there were also 97 million cryptocurrency jacking attacks, 623 million ransomware attacks, and 10 million encrypted threats worldwide.

What gives? Attacks are growing more complex, technology stacks are growing more complicated, and very few can keep up with the speed of digital change.

That's why we are hearing about more incidents and new ways in which old attack patterns are being used. Zero-day exploits, crypto-jacking, IoT attacks, code injections, cloud attacks, and identity attacks are all over the news. And when such attacks hit an organization, the aftermath isn't pretty.

Did you hear about the shutdown of the Colonial Oil pipeline on May 7th? It was a ransomware attack that led to its shutdown after the attackers stole 100 gigabits of data in a two-hour window.

On May 30th, a chemical distribution company was made to pay 4.4 million dollars in ransom via Bitcoin to the Darkside ransomware gang.

Yet another cyber-attack took Channel 9, an Australian broadcaster off the air on March 28th.

It isn't difficult to spot the financial, reputational, and operational spiral into which an organization is thrown down due to a cyber crisis.

For most organizations, orchestrating a communication plan is one of the top challenges when they face a cyber crisis. A part of this problem is not knowing who the relevant stakeholders are, what and when they should say, and to whom.

And, why does this happen? This is because during a cyber crisis, the entire organization is thrown into panic, and inboxes and slack channels start flooding with emails and messages.

Without a response plan, everyone starts replying to them without knowing which ones to prioritize, and how. And you sure as well hope that your communication channels remain unaffected by the attack.

Because cybersecurity incidents can, and very often, do result in network crashes, hacked devices, and data breaches.

With new technologies and tools expanding our digital footprints, the attack surface keeps growing – and because each attack is novel in its approach and impact, a single action plan doesn't help either.

So, is there a way to mitigate this frenzy during times of cyber crises? There sure is!

The first is to build a cyber-crisis communication plan. But how do you do that?

Start by building a cyber-crisis communications committee – this is simply a team of people who will carry out the task of communicating to other stakeholders, including partners, customers, and internal teams of the organization.

Then, identify some of the potential scenarios and have some ready responses to send out to the relevant people in hand. Draft an action plan that tells your teams what tools to use, how to prioritize incoming emails and messages, and the timelines within which they must respond. A good practice is to pick communication channels that can be accessed from anywhere and at any time, and are protected from a potential crisis.

Finally, consider rehearsing for such crises by holding cyber crisis drills. These can help your teams learn about their role in a cyber crisis and if all the stakeholders are on board with your communication and response plan.

The second important step that you can take to mitigate panic during a cyber crisis is to prevent the crisis from happening altogether! This requires you to be proactive in your cybersecurity strategy and to aim for resilience – meaning, you should be prepared for any kind of incident or disruption and be able to prevent it from turning into a disaster.

For this, you must adopt a continuous approach to testing, monitoring, and training when it comes to system security and privacy protection. So, you should not only focus on systems and engage in 24-7 inspections, but also focus on people, by holding cyber drills, tabletop exercises, or call trees.

Another key piece of building cyber resilience is to formulate a crisis management team that can set a crisis management plan in action. Additionally, a cyber-resilience framework will also help you assess your security posture and pinpoint the gaps.

You would have probably heard of NIST's Special Publication 800-160 – Volume 2, which contains extensive guidelines for developing cyber resilient systems. Similarly, IT Governance's Cyber Resilience Framework provides comprehensive information on the governance and management aspects of resilient cyber systems.

Finally, ISO 27001 and 22301 are considered the gold standard in the information security landscape and are leveraged by leading organizations to guide their cybersecurity strategies.

So far, we have looked at two key elements that can help you mitigate the cyber-crisis frenzy: formulating a cyber crisis communication plan and building resilient systems.

The third one is to have the right security tooling in place. With the growing complexity of enterprise technology which spans on-premises infrastructure, multiple public clouds, and edge networks, your organization's security toolset must be able to keep up with this sprawl.

That's why, using cloud-based services that leverage AI, Machine Learning, and automation to fend off cyber threats is a must-have in your cybersecurity arsenal. Consider automating crisis management and response as much as possible to minimize incident response times and eliminate the human factor to seal the possibility of errors wherever possible. In addition to security tooling, having multichannel assistance available at all times can further improve your security posture.

At HCL Technologies, one of our topmost priorities is to arm enterprises against cyber crises. Our end-to-end cyber incident and response capabilities are focused on preparation, detection, eradication, and post-event analysis.

Preparation is about having a cyber-incident response plan in addition to a cyber crisis management plan – and it entails periodic testing and controls audits.

Our threat detection capabilities include AI-based tools that leverage a zero-trust approach and up-to-date threat definition to proactively spot any cyber threats.

Eradication involves finding a permanent fix through application reconfiguration and patching, and post-event analysis aims at finding loopholes and strategizing a mitigation plan.

We continuously explore *what-if* scenarios by assessing potential impact and plan response and recovery activities.

With rapidly evolving technologies, cyber threats are always looming in the shadows. That's why always plan for the worst and take a proactive approach to cybersecurity – this is the key to turning your enterprise into a resilient and secure one.

That's all from today's Cybersecurity Podcast. Thanks for listening, and we hope you found this edition insightful. We wish you a great day ahead.