The Cybersecurity Readiness Podcast

With Dr. Dave Chatterjee

Protecting Academic Institutions from Ransomware and Other Forms of Cyber Attacks

Guest – Garry Scobie, Deputy Chief Information Security Officer, The University of Edinburgh

Summary

Educational institutions have been the target and victim of ransomware attacks. Garry Scobie, Deputy Chief Information Security Officer, The University of Edinburg, spoke at length with Dr. Dave Chatterjee on protecting academic institutions from ransomware and other forms of cyber-attacks. The very engaging and informative discussion covered a lot of ground ranging from identifying the most significant threats to reviewing the challenges of dealing with such threats and making recommendations on how best to secure the academic institution and its stakeholders. Garry shared several good practices, one of which was creating the Champions Network to enhance cybersecurity awareness.

Key Takeaways

(Prepared by Dr. Dave Chatterjee)

Memorable Garry Scobie Statements

- The solution needs to be appropriate, affordable, proportionate, and realistic to the perceived threat level. It is all about taking balanced risks.
- At the end of the day, it is all about the basics and doing them well. The basics are the hardest thing to do and get it right. It is all about people, patches, and processes.
- I am paid to be paranoid.

Single Biggest Threat

- Human-led ransomware is the single biggest cybersecurity threat for educational institutions.
- The trend we see now is that if attackers can get into your network, they will steal your data first, then hack and encrypt the critical infrastructure. They hope the institution will not be able to restore service and be compelled to pay the ransom.
- Attackers gain privileged access by using phishing techniques and then encrypt drives and other critical data repositories.

How Do You Protect the Organization and its People from Ransomware Attacks?

- The solution needs to be appropriate, affordable, proportionate, and realistic to the perceived threat level. It is all about taking balanced risks.
- For this type of attack, endpoint security is critical. The following are some essential defensive measures:
    - Network segmentation
    - Vulnerability management
    - Privileged access management
    - Multi-factor authentication
    - Making sure the remote desktop access protocols are not open to the Internet,
    - Making sure data backups and restoration processes are reliable.
    - Implementing anomaly-based intrusion detection systems to thwart potential attacks.

- At the end of the day, it is all about the basics and doing them well. The basics are the hardest thing to do and get it right. It is all about people, patches, and processes.

How do you cope with the challenges of protecting an academic environment?

- You can do everything possible and yet not be able to guarantee immunity from different types of cyber-attacks.
- You have to engage with the business (i.e., the academic units) and make sure they understand the cyber risks associated with their activities and processes.
- Identifying what is essential and critical to the organization and trying to protect that.
- We cannot let the threat and possibility of ransomware-type attacks destroy the mission and purpose of the academic institution, such as inter-and intra- organizational research collaboration.

Importance of security education and training

- Not having a security awareness program is a threat in itself.
- Security awareness should be looked upon as strategic within any organization.
- We do a great deal of awareness. We are out and about every week talking about the different aspects of security.
- We have created an Infosec Champion's network.
- We have started a newsletter that is gaining popularity within the university community.
- Senior university officials have been very supportive of the security awareness and training programs.
- Academics and researchers often come to me asking, "I want to do this. I found this thing in the cloud. Is it ok to do this from an infosec perspective?" It is excellent that they have come to me and asked for my advice rather than just doing it. This allows me to enhance their security knowledge and awareness further.
- We have put together a 2-page checklist to guide researchers for activities such as:
    - Collaborate and handle research data.
    - Bidding for a research project

- We have created customized information security checklists and shared them with the different colleges and departments. I had all that information available on a website, but it was not being accessed. But getting these checklists in the hands of all the academic units and having them share with their staff and faculty members is a more effective way of raising awareness.

- The checklists are not a list of Dos and Don'ts. It is not about saying what you can't do. It is about guiding them to accomplish their work-related goals without increasing the institution's risk exposure. Essentially, it is about helping academic members make informed decisions.

- The ideal situation is when the customers/user community comes to you (information security personnel) seeking information security guidance.

- If the researcher decides to go with the University supported infrastructure to pursue their initiatives, their actions are protected by professional services. Supported infrastructure greatly assists with complying with the security checklist.

- I am not the gatekeeper for the organization and the business. I don't have the authority to tell the business not to do something. I can advise them on the risk; they can ask for my opinion; at the end of the day, the business must decide what is best for them.

- I am paid to be paranoid.

Securing Students

- It is all about raising phishing awareness.
- We are an open site; we don't have control over student devices.
- We provide lots of advice on what is good practice.
- Students can sign up for my weekly talks on security awareness.
- It is a real challenge, especially with thousands of new students coming in every year and unaware of information security-related best practices.
- We must be mindful of how we communicate to ensure that people from all cultural backgrounds and ethnicities have an accurate and consistent understanding of the message. While communicating humorously might be an effective approach, you must be careful as some may not understand the humor.

- The most important initiative was the **development of a Security Champions network (Champions Network).**
    - An opportune moment due to restricted budgets and impact on recruitment.
    - Developed a pool of staff keen to assist with disseminating our message.
    - We advertised, and almost 50 staff signed up.
    - The Champions Network provides an initial point of contact for infosec queries and to filter assurance queries. The champions promote good information security practices within their school or business unit and share information security materials.
    - The Network serves as a means of communication into schools and colleges. Colleges supported their computing officers with signing up.
    - We have buy-in from the organization.
    - The Champions Network is a staff development opportunity.
    - I believe it does address a need in a devolved environment such as ours.
    - A means of pulling together advice and reaching a consensus.
    - A platform for frank and open discussion.
    - Provides increased visibility of what is happening in schools.
    - Students can also join the Champions Network.
- We hire many students to work for professional services. They learn good security practices and can help to inform their peers.
- We use the highest possible standards to secure vulnerability points.
- Purchased a password manager and pushed it out. Made it freely available to all. The biggest issue we see with students is reusing and sharing passwords.
- I would love to have the finance to install proper endpoint security on their mobile devices.
- Enhance awareness among students. It is surprising how students will have antivirus on their laptops but not on their mobile devices.
- I would love to have the ability to do posture checking when people connect to the network, and I know some American universities have done that on a large scale.

Threats Besides Ransomware

- Not having thoroughly tested your business continuity or disaster recovery process.
- Insider threats, not necessarily malicious ones, but accidental threats?
- Supply chain compromise-related threats.
- Relying on third-party solutions and services.
- The network perimeter has moved entirely since the pandemic hit. Monitoring remote work is challenging.
- Not being able to patch properly or not doing it promptly.
- Organizations will often purchase security solutions but not configure them to their fullest capacity and capability.
- Perhaps social engineering is the biggest threat we all face.
- We can do all sorts of technical stuff to secure networks and data, but protecting people from social engineering attacks is incredibly difficult.

What is a good day for you?

- A good day for me is when my staff effectively responds to security related queries, using the right tone and right measure, and without my help.

Is no news good news?

- I wouldn't say so. Not being aware of something that is brewing and could be potentially dangerous is always a concern. But there is a heightened sense of awareness, and that is the good news. People seem to be getting it and are coming back and asking good questions. For instance, we (CISO office) have constructive and candid conversations with academics who would like to have local administrative rights on their workstations. We recommend against such user access rights because it significantly increases the probability of compromise if the user were to go to a watering hole website.

Are you likely to gain greater stakeholder attention and cooperation by doing a presentation about the different threat scenarios and their consequences?

- People who are not steeped in cybersecurity are unlikely to appreciate the threat impact scenario analyses.
- We once mocked up a newspaper headline stating that we had been attacked and our institutional response to that possible scenario. But it didn't quite have the impact (of heightened awareness) that we had hoped.
- I have carried out Red Team exercises that gave tangible results.
- Red teaming within controlled environments is incredibly useful. It can help focus the organization on immediate problems and vulnerabilities.
- You can't ignore Red Team reports. If you do and you are hit with cyber-attacks, you have nowhere to go.

How do you ensure that intelligence test reports are immediately reviewed and acted upon?

- That is the role of the CISO office. We have excellent lines of communication to ensure that cyber intelligence insights are not ignored.
- We are always in a state of alert. I believe that even when things are going well, we have to be on our toes.

What advice and recommendations do you have for peers at other academic institutions?

- We are not in the business of saying No.
- We must understand and respect the academic mission and culture.
- While institutions can be slow-moving, they have shown great agility when dealing with the pandemic.
- You don't stress about what you can't change.
- I am fortunate that we have good communication links to the top.
- I would look to see what battles I can win while pushing my overall strategy.
- Not waste time on edge cases.

- You need to be an optimist in this line of work.
- Not everyone cares about security as I do.
- My job is to ensure the academic goals and pursuits continue but securely. I can't expect other academic community members to worry about security as they have jobs to do. My job is to identify vulnerabilities and persuade people to adopt the correct security posture.

How do you assess cybersecurity performance at an academic institution?

- Difficult question. Some feel that it would be good to know how many cyber-attacks we stopped this month? I am interested in learning how many cyber-attacks we didn't stop.
- I have three times as many people turning up in my (awareness) sessions this year compared to last year. I have senior staff members attending these sessions.

Any final thoughts?

One of my biggest concerns is IoT. The race to "smartness" comes with many security vulnerabilities and challenges. The genie is out of the bottle. It is happening and the need for security must be addressed now.