What skills does a cybersecurity professional need?

26 November 2018, by Joanne Hall

Cybersecurity professionals work in software development, network testing, incident response and policy development. Credit: Shutterstock

Cyber crime is a threat to every organisation that operates internet-connected devices. It's highly profitable, highly disruptive, and hard to police due to the transnational nature of cyberspace.

Incidences of cyber crime might include fraud, identity theft or privacy breaches, which can have a high personal impact. Ransomware, which locks a system and demands payment, can have widespread economic or healthcare implications.

In the past year, 25% of the Australian adult population was impacted by cyber crime. If we want a robust and resilient society, we need cybersecurity professionals defending every organisation from cyber attack.

Cybersecurity professionals might work in software development, network testing, incident response, or policy development to ensure the security of an organisation.

In popular culture, these experts are often portrayed as lone hackers in hoodies. But in reality, cybersecurity professionals must regularly communicate with a variety of audiences. They must also display a high degree of personal integrity.

What cybersecurity professionals do

To ensure our cybersecurity classes are teaching skills relevant to industry, we consult with security professionals about the skills they are looking for.

As well as technical skills, they tell us they want those they hire to have communication skills, work well in teams, and show empathy and integrity.

The following scenarios show what cybersecurity professionals do on a daily basis. (Names and details have been changed.)

Ensuring systems are compliant

Anna is a software developer for an online retailer. She notices that one of their systems is processing credit card transactions in a way that does not comply with the Payment Card Industry Standards.

The technical project leader does not understand the legal jargon of the PCI standard. The business and legal staff do not understand the software processes behind credit card transactions.

It's Anna's job to bring together technical, legal, and business operations staff to discuss the resources required to fix this problem.

Identifying vulnerabilities

Basim is a security specialist working for a consulting company. His team has been contracted by a superannuation fund to conduct a simulated attack on the fund's network.

Basim's team grabs a round of coffees and sits around the whiteboard to develop a plan. That afternoon they find a way to change the password of every customer, using a commonly known

vulnerability.

Basim immediately calls the super fund to notify them of the dangerous vulnerability. He then spends the rest of the afternoon working with the super fund's IT team to begin to fix the issue.

The team continues with the simulated attack for three more days and finds a few (less urgent) vulnerabilities. The team collates the attack notes and writes a comprehensive report. The next day Basim hands over the report and delivers a presentation to key members of the super fund.

Monitoring and responding to attacks

Chiyo works in the Security Operations Centre of a university. Her team has set up monitoring systems that alert them to any malicious software (malware) on the university network.

The monitoring system alerts her to some unusual activity with a staff email account, and automatically disables that account. She investigates and finds that a staff member has opened an email attachment containing malware.

Chiyo calls the staff member to notify them that their account has been disabled and discusses the process to regain access. A member of Chiyo's team configures the email filter and firewall to block the source of malware.

Meanwhile Chiyo walks over to the staff member's office and erases all data on the infected computer. She then works with the staff member to reinstate the email account, set up software, and retrieve documents from backup storage.

Preventing data breaches

Dimitry works in the cyber security team for a government department. His team is asked to analyse the policies, procedures, and structures of the department to look for risks to citizens' privacy. He discusses the current laws and best practices with a colleague from the Office of the Australian Information Commissioner.

Dimitry's team identifies five processes where there is a high risk for personal data to be leaked. They analyse each process, determine the likelihood of each type of problem, and examine the possible outcomes of each risk scenario. Dimitry develops a plan and budget to reduce each of the risks. He presents a report to the Minister and the Department Secretary.

The Department Secretary determines that there is a strong case to implement the plan for two of the risky procedures immediately. The other three risky procedures are deemed low-priority, and will be re-examined in six months' time. Dimitry sets up a team to implement the remediation plan.

Integrity and communications skills are essential

These scenarios highlight that, in addition to their technical skills, cybersecurity professionals need to work in teams and communicate with a variety of people.

In each case, the security professional had access to information that could easily be sold on the black market, or exploited for personal gain. Anna could have stolen credit card details. Basim's team knew about some vulnerabilities three days before they informed the super fund. Chiyo had access to a staff member's entire email history. Dimitry knows about three vulnerable processes that will not be changed for six months.

Personal integrity is crucial to maintain the security of these highly sensitive systems.

Communication with non-technical staff is essential to ensuring that best practice is implemented across an organisation. A strong ethical framework is an absolute necessity for security staff. The best technical staff will only build a safer organisation if their communication skills are strong and their personal integrity is unwavering.

Provided by The Conversation