

INFO5990: Professional Practice in IT

Week 8: Security Management

Dr. M Sajjad Akbar

School of Computer Science

“Whether greater cybersecurity requires a greater sacrifice of our digital freedoms is an important debate that we should be having, preferably with all the facts in front of us”.

Evgeny Morozov



THE UNIVERSITY OF
SYDNEY

Overview

- Part A
 - Security Management
 - Not focusing on:
 - Security tools / Techniques
 - Rather, focusing on:
 - Appreciation of the importance of managing security
 - Understand the sort of difficulties encountered in security in large software systems
- Case Studies
- Discussion...

The Optus hack will cost millions (and not just in payouts)

Based on the experience of companies overseas, the Optus cybersecurity breach could cost the company hundreds of millions of dollars.

Sep 23, 2022 – 6.54pm



Save



Share

The minor move in the share price of Singapore Telecommunications, the parent of [cyber-hacked telecommunications company Optus](#), is surprising given the likely heavy commercial costs from losing the data of up to 9.8 million customers.

Optus will suffer financial damage in two ways. It will lose profits to competitors as existing and potential customers go elsewhere. Also, its expenses will balloon to cover the cost of fixing its weak security defences and to compensate customers.

<https://www.afr.com/chanticleer/the-optus-hack-will-cost-millions-and-not-just-in-payouts-20220923-p5bkkm>

Security: The TJX case: 17 Jan, 2007

- TJX retailers
 - 2100 stores in US, 300 in Canada
 - \$16 billion annual revenue
- “The worst retail **data breach ever?**”
 - **46 million customers affected**
- Details
 - What happened?
 - How did it happen?
 - What was the result?
 - What lessons?



Timeline of TJX investigation (1)

- 18 December 2006, suspicious software discovered on TJX network
- 17th January 2007 TJX reported unauthorised access to credit card information stored on their network
- March 2007 TJX admitted to possible breaches having occurred as early as July 2005
 - Since data was stored unencrypted and held long-term transactions, as far back as 2002 could have been affected
 - Potentially 45.7 million accounts compromised.

- Hackers sold 80GB data to thieves
- Fake credit cards used to purchase gift vouchers. Losses experienced by card companies US\$50-100 million.

Timeline of TJX investigation (2)

- Mar 2007 six suspects arrested
 - Irving Escobar, age 18; Reinier Camaraza Alvarez, 27;
Julio Oscar Alberti, 33; Dianelly Hernandez, 19;
Nair Zuleima Alvarez, 40; Zenia Mercedes Llorente, 23
 - Charged with “organized scheme to defraud”
 - Bonds set at \$1 million each.
- 8th May 2007 TJX revealed that the fraud had probably been via Wi-Fi. Data was intercepted before it had been encrypted. Thieves also had the key.
- Sept 2007 Irving Escobar sentenced to five years jail
- October 2007 - TJX fined \$880,000
- November 2007 - TJX settles with Visa for **\$40.9M** to cover the costs of reissuing the cards.
- April 2008 – TJX settles with MasterCard for \$13M

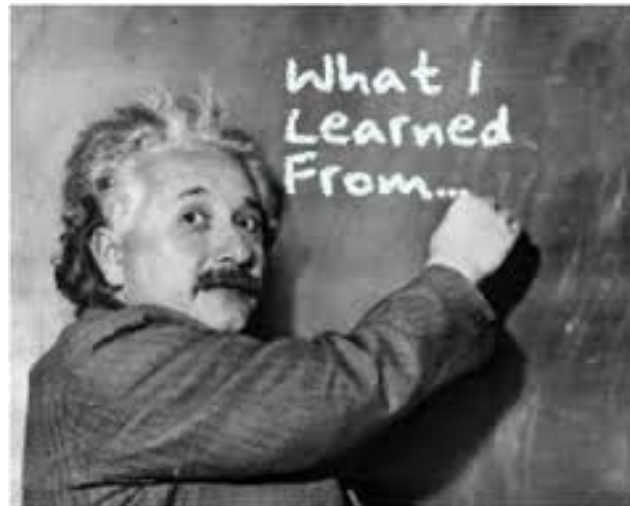
Aftermath

- August 2008, 11 men charged with hacking into nine U.S. retailers, including TJX.
- March 2010, hacker Albert Gonzalez pleaded guilty. Sentenced to 20 years in prison .
 - the lengthiest punishment ever imposed for computer or identity theft crimes
- 8 May 2010, Ukrainian Sergey Storchak arrested in India on his way home.



What can we learn?

- Need to take care with data
- Data is a saleable commodity – WHY ?
- Follow rules for our own protection
- Criminals are getting smarter
- Consider use of encryption



Australian Computer Crime & Security Survey

“The Morrison Government estimates cybersecurity incidents cost Australian businesses \$29 billion each year. People lost an average of \$700 to cybercrimes, according to survey results released mid-2019.”

<https://www.aic.gov.au/publications/sr/sr43>

<https://www.emergingit.com.au/insights/the-hidden-costs-of-australian-business-cybersecurity-lapses>

- **Credit card skimming**
- Identity theft
- Computer scams
- False passports
- Money laundering

*** Australian High Tech
Crime Centre**
**† Australian Computer Emergency
Response Team**

Types of crime, abuse experienced

- External attack greatest threat
 - attacked externally, internally.
- Form of crime or abuse
 - laptop theft
 - virus or worm infection
 - trojan or rootkit attack(root access)
 - denial of service attack
 - unauthorised access



Factors thought to contribute to vulnerability

- Unpatched/unprotected software
- Inadequate staff training
- Poor security culture
- Misconfigured software



Security Management Frameworks

– ITIL

- ITIL Security Management (IT Infrastructure Library)
- ITIL is a framework with a set of practices for IT activities such as IT service management (ITSM) and IT asset management (ITAM) that focus on aligning IT services with the needs of the business.

- https://en.wikipedia.org/wiki/ITIL_security_management

– COBIT (Control Objective for Information and Related Technology)

- Provides structured set of practices and Principles (Risk management, Governance, Compliance etc.)

- <https://miroslawdabrowski.com/downloads/COBIT5/COBIT%205%20-%20Cheatsheet%20%5bv1.0,%20Minimarisk%5d.pdf>

– NIST (National Institute of Standards and Technology) Cyber Security Framework

- https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

- 5 functions (comprising 23 categories)
- Identify (e.g. Business Environment; Risk Assessment; ...)
- Protect (e.g. Access Control; Data Security; ...)
- Detect (e.g. Anomalies and Events; Continuous Monitoring; ...)
- Respond (e.g. Analysis; Mitigation; ...)
- Recover (e.g. Recovery Planning; Improvements; ...)

Aspects of security management that are proving to be a challenge

- Difficulty of changing attitudes of users to security
- Keeping up to date with threats
- Configuration management
- Lack of understanding by senior management
- Lack of commitment by senior management

Cost of computer attacks on Australian organisations in 2024

- In 2024, cyberattacks imposed significant financial burdens on Australian organisations, with the average cost of a data breach reaching **AUD \$4.26 million**, marking a 27% increase since 2020. [SecurityBrief Australia](#)
- This escalation reflects the growing complexity and frequency of cyber threats, including ransomware, phishing, and AI-driven attacks.
- Notably, the Australian Signals Directorate (ASD) reported that small businesses faced an average loss of **\$49,600 per cybercrime incident**, an 8% rise from the previous year. [Cyber.gov.au](#)
- These figures underscore the critical need for enhanced cybersecurity measures across all sectors.

Spending on security by Australian companies

- 66%
 - of respondents reported that they spend between 5 and 10% of IT budget on security
- **Software controls**
 - Anti-virus software
 - Firewalls
 - Anti-spam filters
- **Security management procedures**
 - Media backup
 - System security audit
- **Encryption technologies**
 - encrypted login/sessions
 - encrypted files

Reporting incidents to law enforcement

- 22% reported the incident
- Notifiable Data Breach (NDB) scheme part of Australian Privacy Act 1988 (Govt, Healthcare, personal info, credit reporting bodies, tax file number recipients, private sector > 3M revenue)
 - 69% of those affected chose not to report – why ?
- Reason given for not reporting
 - Not considered serious enough
 - Didn't think perpetrators would be caught
 - Didn't think authorities were competent
 - Wanted to avoid negative publicity
- Outcome where reported
 - No charge due to lack of evidence
 - Not investigated
 - Charges laid



Data breaches

- See <https://www.webberinsurance.com.au/data-breaches-list>



Malware as a threat to information security



According to Wikipedia: Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, and other malicious programs.

It can take the form of executable code, scripts, active content, and other software.

The Anti-virus industry

- Examples: Norton, McAfee, Microsoft
 - Symantec Corporation Revenue \$6.9 billion, Net income \$814 million. Norton Anti-Virus costs \$54.99 per year
- The number of potentially malicious threats emerging each month has increased from 300 in 2003 to 9,200 in 2020
- An unpatched computer with neither antivirus nor firewall protection has a 50 percent chance of becoming a zombie within 30 minutes of being connected to the internet.
(Sophos, 2006)



MyToll still down after ransomware attack

Toll Group says it's slowly bringing IT systems back online.

By Casey Tonkin on May 12 2020 10:10 AM

[Print article](#)[Tweet](#)[Share 1](#)[Share](#)

Logistic company Toll Group is still not fully online following a ransomware attack that brought down its IT systems last week.

In an update yesterday afternoon, Toll said it was bringing its systems "progressively online" after one of its "core IT systems" was securely reactivated last week.

"At the same time, we're continuing to support our large enterprise customers whose services are affected by the disruption to online operations," the company said.

"While there are delays in some parts of the network, freight shipments and parcel deliveries are moving by and large as normal, with Toll call centres taking bookings over the phone."



Toll Group is working through its second ransomware attack of 2020. Image: Toll

Computer crime and the law



What is cyber crime ?

Can we win the fight against
cyber crime?

Privacy Act 1988 vs Cybercrime Laws

Area	Law	Purpose
Data Privacy	Privacy Act 1988	Protects personal information
Cybercrime Offences	Criminal Code Act 1995 (Part 10.7)	Defines and penalizes cybercrimes
Surveillance and Investigation	Surveillance Devices Act, TIA Act	Governs lawful access and monitoring
International Cooperation	Cybercrime Act 2001	Aligns with global cybercrime frameworks

Australian Cases

- **1995: Skeeve Stephens**
 - Stealing and publishing credit card details
 - 3 years jail
- **2000: Vitek Boden**
 - Hacked into Council computers and released millions of litres of raw sewerage
 - 2 years prison
- **2008: Bradley David Ward**
 - Hacked into council computers “out of curiosity”
 - Fined.
- **2009: David Anthony McIntosh**
 - Hacked NT government systems. \$1.2M worth of damage
 - 2 years jail
- **2013: Matthew Flannery (“Aush0k”)**
 - Numerous hacking offences
 - 15 months home detention
- **Various: Julian Assange**

Five categories of security threats

1. Unintentional acts

- Human error, carelessness, ignorance

2. Natural disasters

- Power outage, fire, flood, earthquake

3. Technical failures

- Hardware failure, software failure

4. Management failures

- Ineffective procedures and controls

5. Deliberate acts

- Vandalism and malicious damage

Protecting data

- Privacy
 - should you store this data?
 - what is it for? is it all necessary?
- Accuracy
 - is it correct, complete and current?
- Property
 - who owns it? can it be sold to others?
- Accessibility
 - confidentiality: who has access to the data?
 - when and for what purpose may it be used?

Factors making security harder

- More complex systems, distributed data, unmanaged devices
- Criminals becoming cleverer: more and more threats
- Crimes often not detected for long periods
- Wide range of users, mostly non-expert
- Management unaware of problems
- Security measures often inconvenient
- Costs substantial
- Benefits hard to quantify

Other major sources of risk

- IT department employees
- Human Resources department employees
- Managers
- Consultants
- Cleaners
- Outsiders, hackers etc
- ‘Social engineering’



The biggest security threat of all: Users!!

- Leaving the door open – logged on
- Laptops
 - Over 600,000 laptop thefts occur annually in the US
 - Estimated USD\$5.4 billion loss of proprietary information
 - Over 90% of these laptops are never recovered
- Lack of care with passwords
- Opening dodgy emails
 - Test yourself: <http://www.sonicwall.com/phishing/>
- Careless internet surfing
- Use of portable and unmanaged devices
- Discarded materials and equipment



‘Business continuity’



**The last resort:
Backup and recovery**

Business Continuity Planning and Management

- iDRP and BCP
- Every year 1 in 500 businesses will experience a severe disaster
- 43% of businesses that experience disasters never re-open
- 29% close within 2 years

<https://www.youtube.com/watch?v=1V1SCWOXJbc>

(Source: McGladrey and Pullen www.continuitycentral.com/feature0660.html)



Business Continuity Management

- Organisation should be able to continue to function during a disaster, rather than simply trying to recover after a disaster has occurred.
- The aim is to come out of an IT mishap relatively unscathed and with little or no impact on your clients or your business.

smh.com.au/articles/2003/10/13/1065917329798.html and
www.johnglennrcrp.0catch.com/quotes.html

Planning for business continuity

- Backup procedures
 - Routine backups
 - Adequate, complete, incremental
 - Mirroring
- Disaster recovery
 - Data, equipment, people
 - ‘Hot’ sites
 - Practice
- System audit

Case Study: Aust. Stock Exchange Business Continuity Testing

Participants are advised that from 7 February to 11 February 2016, ASX 24 and ASX Clear (Futures) will be undertaking a **comprehensive test of the Business Continuity capabilities** of its core systems.

ASX Bridge St core system infrastructure will be configured as standby for redundancy purpose.



Malware attacks

- Kinds of attack
 - Denial of service - emails and spam
 - Clandestine acquisition of data - trojans
 - Zero-day attack - specific actions
 - Phishing attack - using email to steal personal data
- Kinds of malicious software
 - Replicating – denial of service
 - Non-replicating – spyware: new trend towards financial gain as motivation

'Phishing'

- The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
 - The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, and bank account numbers
 - Example (2003) : e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the link provided



Is the email really from eBay, or PayPal, or a bank?

As an example, here is what the email said:

- Return-path: <service@paypal.com>
- From: "PayPal"<service@paypal.com>
- Subject: You have 1 new Security Message Alert !

Note that they even give advice in the right column about security



Test yourself:

<http://www.sonicwall.com/phishing/>

From: "PayPal" <service@paypal.com>
Subject: You have 1 new Security Message Alert !



PayPal Security Center: Urgent PayPal Account Login Request.

Notice of account temporary suspension

Dear **PayPal** member :

- We regret to inform you that your **PayPal account**, has been **temporarily blocked** due to various login attempts from different global locations.
- As **Romania** is one of the most high rated fraudulent countries, we temporarily **blocked** your account to avoid future problems or misuse of your **PayPal** account.
- Here are the last 3 login attempts :

How to protect your account

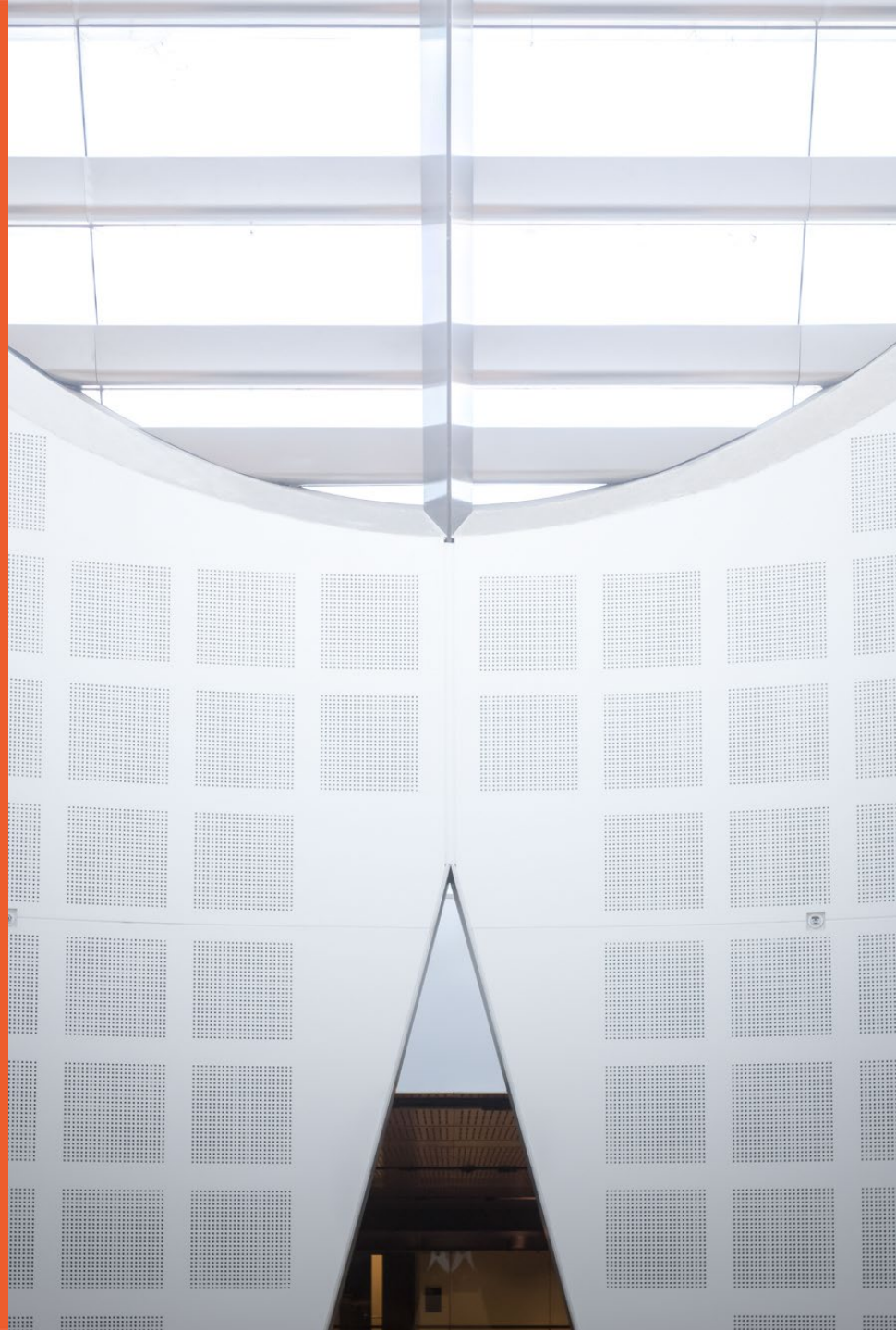
- Make sure you never give away your PayPal login and password, to someone you don't know.
- Please respect PayPal policy and privacy statements. For more information on how to protect your account, please visit our security center.
http://www.paypal.com/cgi-bin/cmd=_security-center-outside

INFO5990: Professional Practice in IT

Week 8: Optus...



THE UNIVERSITY OF
SYDNEY

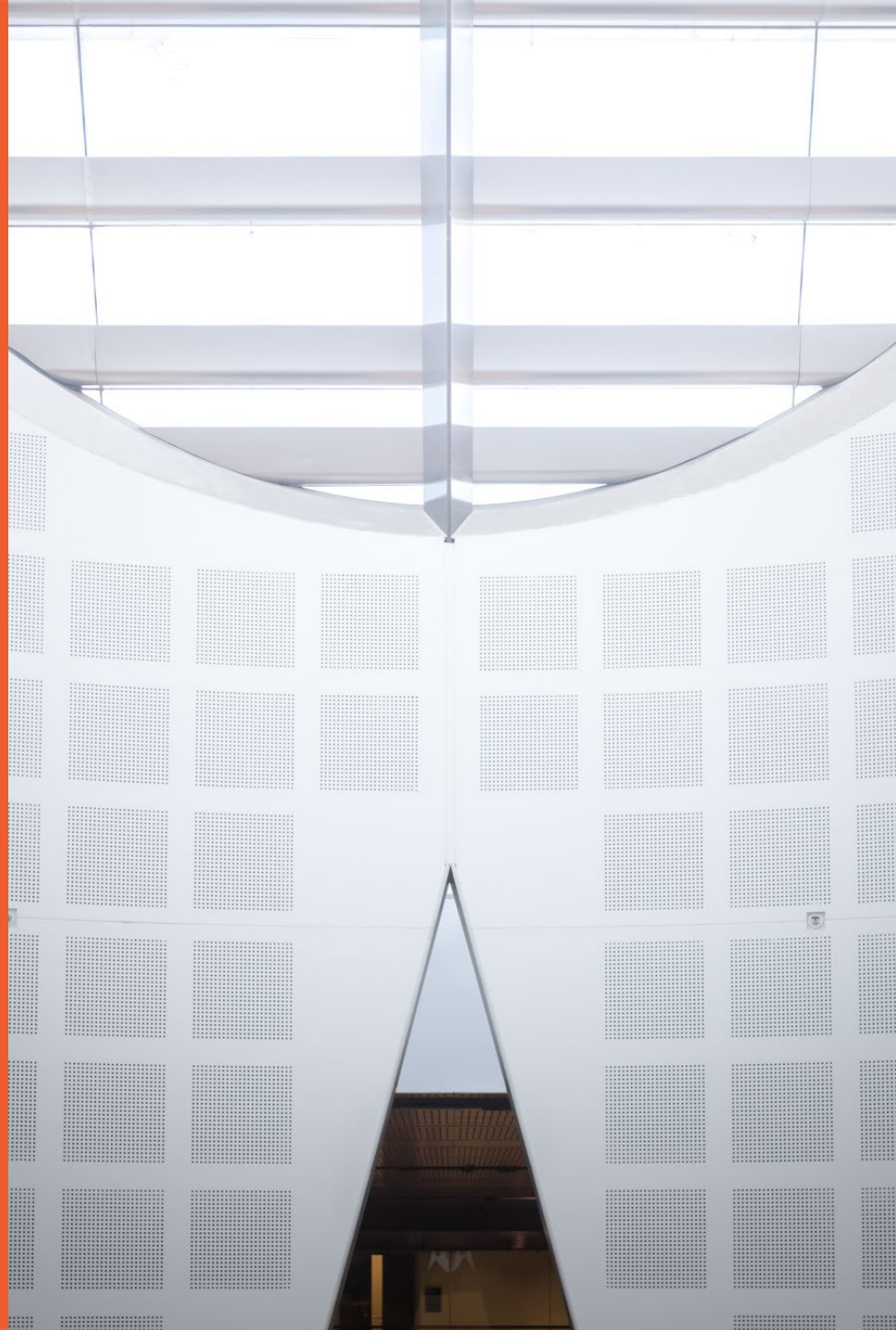


INFO5990: Professional Practice in IT

Week 8: Discussion



THE UNIVERSITY OF
SYDNEY



Questions

1. What are the biggest cyber security threats currently?
2. Who should be responsible for managing security?
3. At what level of a company does this need to be understood?
4. What proportion of a project budget would normally be spent on security?
5. (And on what things would that budget be spent?)
6. Can you be 100% secure?
7. What is a pen test or penetration testing?

- <https://www.tetradefense.com/cyber-risk-management/15-cybersecurity-questions-to-ask-for-c-suites/>
- <https://www.guru99.com/cyber-security-interview-questions.html>