Cyber Security
An Industry View

Understanding The Risk is the First Step towards Reducing it

David Cahill

Security Strategy and Architecture Manager

AIB

CISSP®
Certified Information
Systems Security Professional

AGENDA

- Threat Landscape
- Challenges
- Approach
- Data Protection Controls Sample
  - DLP
  - Ransomware vs Targeted Ransomware
  - Threat Intelligence
  - Phishing
  - Access Control
  - Compensating security controls to your estate
  - Deception / Honeypots
  - Testing

Changing Threat Landscape for Financial Industry

Traditional: “I want your money”

- Money was typical physical
- Physical protection was the main focus

New: “I want your money and/or your data”

- Physical protections are still required
- Virtual protection requirements are increasing
- Money has increasingly shifted to become data (01101101 01101111 01101110 01100101 01111001 = Money)
- Personal data has increasing value/obligations

Threat Samples

Physical Threats

“The 10 Most Successful Bank Robberies In History”

1. **Banco Central Burglary Brazil 2005 : $70m**
2. **Brink's-MAT Robbery UK 1983 : £26m** 🧍
3. **Securitas Depot Robbery UK 2006 : £53.1m**
4. **Northern Bank Robbery Belfast 2004 : £26.5m**
5. **Central Bank of Iraq; Iraq; 2003 : >$920m** 🧍
6. **British Bank of The Middle East; Lebanon; 1976: $20-50m**
7. **Knightsbridge Vault Robbery; UK; 1987: £62m**
8. **Dar Es Salaam Bank; Iraq; 2007: $282m** 🧍
9. **The Great Train Robbery, UK; 1963 £2.6m**
10. **Dunbar Armored Robbery; US; 1997: $18.9m** 🧍

Source: thrillist.com

Bank of Ireland; Dublin; 2009 €7.6m

🧍 ***= Insider involvement***

Virtual Threat Examples:

- Most Virtual threats are “high volume, low value” but high value thefts still occur
- In 2016, cybercriminals hacked into the SWIFT system using stolen credentials. They made requests to the Federal Reserve Bank of New York for $1 billion to go from Bangladesh’s central bank to accounts in the Philippines and Sri Lanka.
  - If it wasn’t for a Typo in one of the transfers (caught by an intermediary bank) this could have been larger that any previous Bank theft in history. $81m was transferred before the error was spotted.

How big is the “virtual” Threat?

- Hacking groups continue to grow and have enormous resources at their disposal
- Sample “The Dark Overlord”
  - The Dark Overlord is a online extortion gang that regularly steals data and then attempts to ransom it back to victims.
  - Anyone who doesn't comply gets threatened with the full data set being leaked
  - The group often try to increase the pressure on victims by trickling out the stolen data

Source: cyberscoop.com

Sample Activity of this group: (Jan 2019)

- The **DarkOverlord** claimed it had **stolen emails, retainer agreements, nondisclosure agreements, litigation strategies, liability analysis** and other information that would embarrass high-profile insurers **Lloyd’s of London and Hiscox Syndicates as well as Silverstein Properties**, a New York real estate firm.
- The Dark Overlord claimed to steal more than 500,000 records.
- Material was published on Thursday (4th Jan) representing what the Dark Overlord described as the least sensational documents.
- The Dark Overlord announced it would publish the stolen material in five data dumps unless escalating payment goals were met, from $5,000 worth of bitcoin to $2 million.
- Hiscox confirmed **a law firm that advised the company had experienced a breach**.

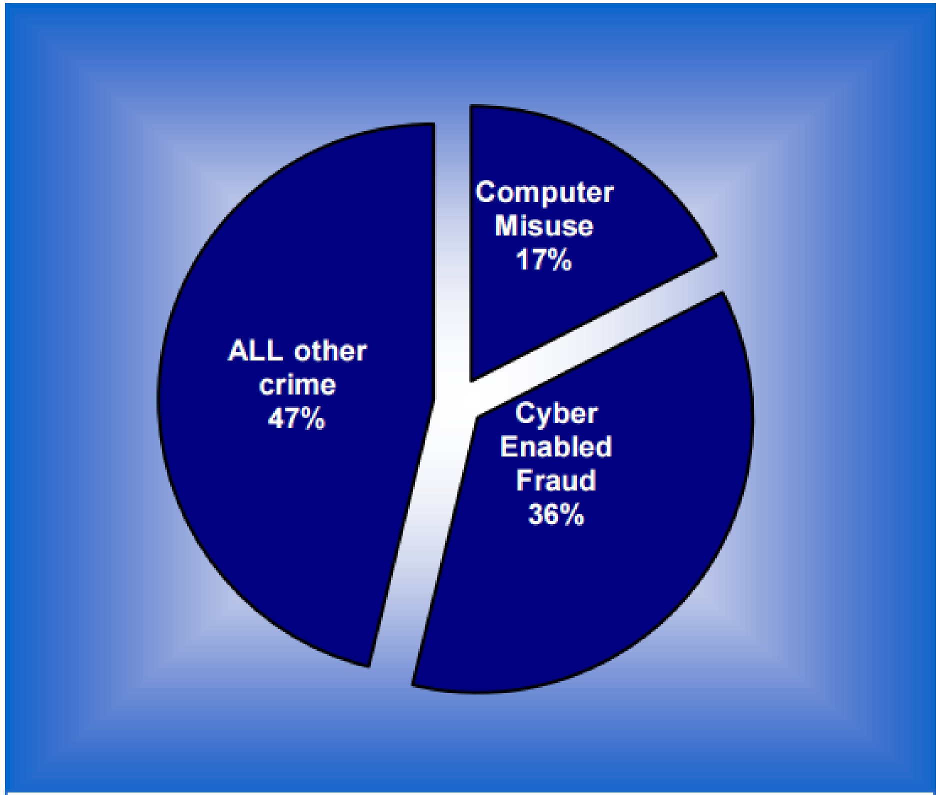
And it’s getting “mainstream”

- Nov. 14, 2018, “The Dark Overlord” posted as a job advertisement on KickAss Forum - a cybercriminal marketplace on the dark web:
- ***“Do YOU want to get Rich? Come work for us!,”***
  - *“You’ll be working in a strong team-based environment, communicating and collaborating with like-minded and ambitious individuals,” …… “You’ll be checking into project trackers, accepting suitable workflow positions, and carefully documenting your work for review. You’ll be engaged in operations against various companies and governments and world-wide deployments. If you’re goal-oriented and used to objectives and achieving them, then you’re perfect for us.”*

“Must have a very good ability to document your workflow and formulate articulate reports on your duties”

*“New employees would be paid **($63,500) monthly**, plus add-ons and a likely pay bump up to $89,000 monthly after two years.”*

How big is the “virtual” Threat?



Cyber Crime as a proportion of total UK crime in 2015 (Source: ONS)

Source: https://www.nationalcrimeagency.gov.uk

- **Cyber crime overtook “traditional” Crime in the UK in 2015**
- *“The ONS* (Office of National Statistics) *estimated that* ***there were 2.46 million cyber incidents and 2.11 million victims of cyber crime in the U.K. in 2015****”*
- ***“Data breaches are among the most common cyber crimes committed*** *against businesses.*
- ***“Almost all large companies and a substantial majority of smaller companies have experienced a data breach****.”*
- *“Meanwhile,* ***cyber-enabled fraud*** *– most commonly, but not exclusively, targeting retail customers –* ***is a rising cost for banks, retailers and other businesses****.”*

New Regulations bring New problems

- “Jake Moore, cyber security expert at ESET, predicts 2019 will see a new form of attack: **GDPR bounty hunting**.”
  - “GDPR bounties work effectively when the attacker extorts an organization by providing them with a copy of their data to prove that it has been breached.
  - "They then give the victim two options: pay the possibly eye watering ICO fine of up to €20m or 4% of their annual global turnover – or pay the hackers’ chosen fee, which could be anything less than the maximum from the ICO. Hackers take advantage of the fact that some organizations will be tempted to choose the second option so they can avoid any reputational damage caused by a data breach.”

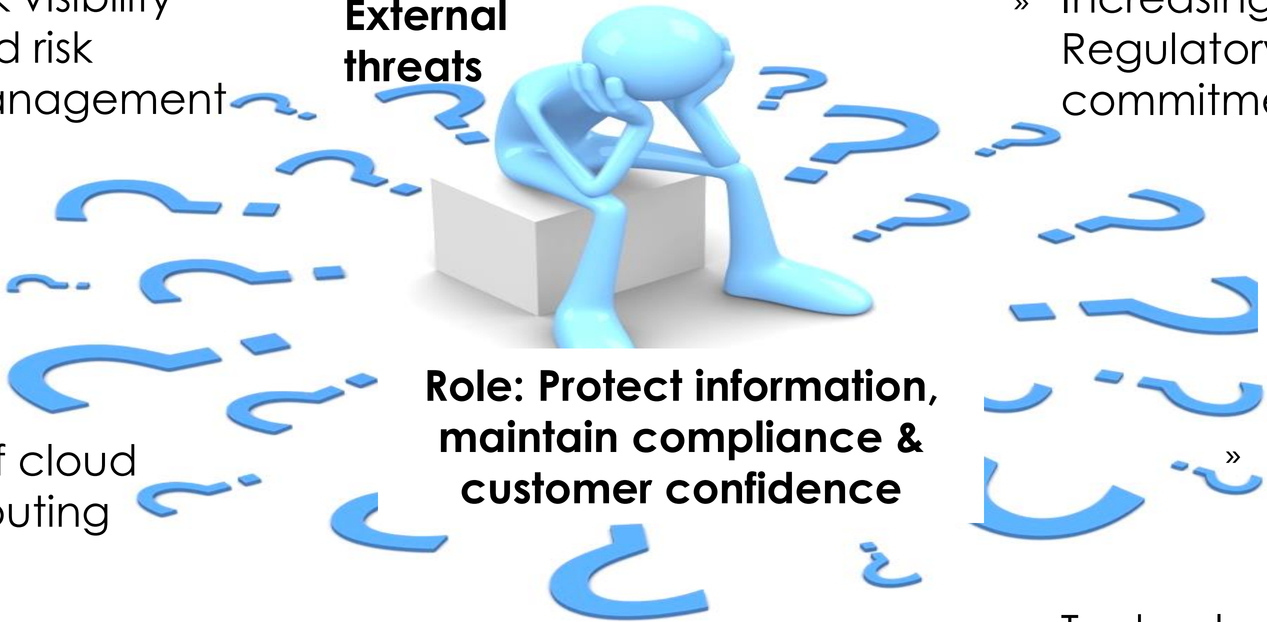
Source: forbes.com Dec 2018

- This is actually nothing new – Hackers extorting Victims for money. However it could be construed that GDPR fines provide hackers added leverage against victims with weaker security posture.

Today’s Cyber Security Challenges Overview

“And Stay awake! – it will all change tomorrow”

- Risk visibility
- and risk management
- **Increasing External threats**
- Internal threats
- Increasing Regulatory commitments
- Balance usability, risk, and cost
- Increasing Business Agility Requirements
- Technology to efficiently collaborate with partners and customers
- 1000’s security vendor products
- Outsourcing to deliver cost effective services
- Dissolving security boundaries
- Use of cloud computing



Role: Protect information, maintain compliance & customer confidence

Quick Relief:

Stress Reduction

Bang Head Here

Directions:

1. Place on FIRM surface.
2. Follow directions in circle.
3. Repeat step 2 as necessary, or until unconscious.
4. If unconscious, cease stress reduction activity.

Cyber Security Approaches:

Ignore –unfortunately often used

Not an option for a highly regulated environment!!!

Recent regulation (i.e. GDPR) makes this approach less acceptable

Deal with it & be realistic:

- Cyber Security is a Journey – not a destination
  - Not everything can be solved immediately
  - Newer and more advanced threats are constantly emerging
    - Review Regularly but don’t get distracted
- Others are taking that journey also
  - Share knowledge with industry peers
  - Use proven frameworks that are relevant

What Do We need to do?

Protect Against Risks

- Data Loss
- Financial Loss
- PR Damage
- ….

i.e.:

- Protect our Customers

Comply With Regulations

- Data Protection
- Audit Trails
- Transaction Records
- …..

i.e.:

- Protect our Customers

Approach
Use a Good Baseline

Security Frameworks Exist

- ISO 27000
    - Non-Industry Framework that covers Security Controls and Standards
- Create Organisation level Policy & Standards to minimise risk across all areas
- Review Regularity Requirements
    - PCI-DSS
    - SOX
    - Data Protection (GDPR)
    - …
    - Update Policy & Standards as necessary

Approach
IT Department as “leaders”

- Never Ending list of new security technology & Controls
    - Anti-Virus
    - Firewalls
    - Data Backups
    - Sever Hardening
    - Encryption
    - SIEM
    - MFA
    - …….

- All provide layers of protection but
    - Costs of each protection layer
    - Complexity of each layer
    - Effectiveness of each layer
    - Technical Reps = Technical centric controls = usability issues and user resistance

Approach
Risk Management as Driver

- Risks reviewed using stakeholders from across the organisation
  - Including staff that will utilise the solution is key to ensure usability of the control.
  - They often know more about the data that the IT staff.
  - Often these staff are not security knowledgeable, but good security controls shouldn’t require a expert (you don’t need to be a mechanic to drive a car)
  - Ensures that Risk and mitigation is owned by ALL relevant stakeholder– not just pushed to being another IT problem to solve in a silo.
- Risks Recorded and prioritised to reduce risk with available resources
- Better buy-in for need and use of controls
- Ensures controls are fit for purpose and are usable
- Controls can be technical, but often are a mix of People, Process and Tech

- Result: Better design and better protection

Protecting the virtual Data

- Data Loss Prevention (DLP) Strategy is Key
  - Loss can be malicious or accidental
  - Technology controls are not the answer by itself (People, Process & Technology)
- People
  - Education is Key
    - Awareness of Responsibilities
    - Awareness of Threats
    - Awareness of Controls
- Process:
  - Least Privilege Approach (who needs access to the data – what if they are breached)
  - Segregation of Duties
  - Data Classification
- Technology: ALL Data Channels require protective controls to prevent loss.
  - Data Storage / Servers
  - Data Access Mechanisms
  - Email
  - Web access (Uploads)
  - Client devices (Laptops, USB keys etc)
- Continually review and improve protection and re-educate

DLP (Data Loss Protection)

- The importance of data loss protection to an organisations integrity, reputation and financial operation [GDPR]
    - Security Controls & Advances in external intrusion prevention are often the main focus of cyber security within a firm.
    - However, often more and more threats to data integrity and threats come from within your organisations perimeters.
    - This include your key vectors including employees. Sending emails from within your organisation often to external resources , containing possible confidential company, client and/or IT System Design documentation.
    - Whilst not always with malicious intent, users/employees can open your organisation up to attack, sanction, penalty (data loss) and or fines.
    - An example of this would be a sweeper for DLP installed on your email environment and or alternative mail routing tools which will trigger policies based on headers, based on recipient lists and the contents of the body and attachments of that email.
    - With the appropriate triage and responding teams/procedures in place. You will build a strong defence from within to maintain your data, and the hygiene of that data.

DLP Channel Control Sample - Email

- What are we trying to protect?:
  - Sending of data files that contain customer account data or confidential information

- Rule on email Gateway (DLP capable) (Technical Led):
  - **Block** outbound that contain “IBAN pattern” or “CC Number Pattern” or “…” (and Alert SOC, Line Manager etc…)
  - The above simple rules help block the data leaving but inhibits legitimate customer/partner communications on the channel.
  - Disable Control? ☹

- DLP Process, People and Technology (Risk Led):
  - Consider who has legitimate reasons. Can they use a “proxy” person instead? (i.e Only “Bob or Sarah” can send those types of emails…..)
  - Additional higher priority rule:
    - **Encrypt & Quarantine** outbound emails that contain “IBAN pattern” or “CC Number pattern” or “…” (and LOG) when from department (or user) “xxx”
  - Quarantine Release Process
  - Result: > 90% of internal systems/users (or malware) preventing from bypassing standard DLP controls while mechanism for legitimate business use.

DLP (Data Loss Protection)

- Vendor controls
  - Often when organisation employ a vendor to carry out a piece or work or outsource a function from within their organisation. Appropriate controls should be put in place, to ensure that the vendor in question, has control and access to carry out “ONLY” the activity and/or procedures that has been asked of them. In most cases segregation of duties clearly defines this.
  - However, in the interest of clarity and some example of that would be:
    - RBAC – Role Based Access Control
      - Allowing users to do only what their role defines them to do
    - Logon Hours
      - Ensuring vendors access to your network is defined within the requested hours of service
    - Learning:
      - Understanding what is “Normal activity” for your vendor, so that if any activities outside the duties clearly setup for them will be identified and flagged as “suspicious” and investigated
    - EDR
      - In some cases, organisations may use internal Endpoint Detection Response technology to identify activities conducted and movement within a network if any of the above occur/are not followed

Ransomware vs Targeted Ransomware

- Shift in behaviour from pre-2016 Ransomware attacks to post-2016 targeted ransomware attacks
  - Ransomware attacks have drastically shifted within the last 4 years from "Generic ransomware attacks"
    - Mass emails are now quickly being picked up and filtered by major email filtering systems
  - Targeted Ransomware:
    - Use of Social Media to determine "key targets"
    - i.e. "John" has posted on his linkedin profile he is "Database Admin @ Company X"
    - "John" has also posted that he is attending a Fintech Seminar in July
    - Attackers send John an email pretending to be event organisers with an updated Agenda as attachment.
    - The Attachment contains "one-off" modified malware payload making it less recognisable to Security tools.

Ransomware vs Targeted Ransomware

- Phase 1: Recon & Lay dormant
  - After successful delivery of a payload, attackers often leave their ransomware idle and go undetected. in an effort to learn and map out mission critical platforms/servers and spread to were most effective in causing impact.
    - In some cases, ransomware was seen to go undetected for 18 – 24 months prior to be activated across an estate,
  - Phase 2: Activate 16-18 months: Once activated in this case, Ransomware can cripple your infrastructure and network bringing your operation to a complete halt.

  - Having an appropriate SOC and Major Incident Response team to deal with this event is key to the business continuity of your organisation. Standard operating procedures and all appropriate vendor roles refined.

Threat Intelligence

- Logs, Events, SIEM, data analytics
  - Logging all events, authenticated attempts and activity in your network is key.
  - Provides better ability to detect abnormal behaviour over time.
  - How to control that activity, make for a more secure environment and giving you full insight into how your stakeholder manage and operate their IT operate estate.

Threat Intelligence

- IR & EDR response
  - Incident Response
    - Managing the incident response to this type of attack is critical to the quarantining and isolation of infection if time and escalation paths are followed. If internal or external, an IR team conducting Triage, Escalation, Engaging stakeholders and isolating a malicious activity is key to limiting damage to your estate.
  - Endpoint Detection Response
    - EDR technology allows you to identify infected devices and reverse engineer the attack which took place in an effort to identify how the attacker got into your network to patch, remediate or otherwise close any gaps or quarantine devices from this payload initiating once again. This type of activity is also key to learning more about the attack and how the attacker exploited your security controls and toolsets. Additionally, the sharing of this information between policing authorities will help mitigate future attacks and/or resolve them in a more timely fashion

Phishing

- Your employees are your first line of defence, educating your employees to protect your organisation
    - Too often, we see successful Phishing attempts occur within organisations, resulting in loss of data, intrusion and loss of credentials such as passwords, data and more significantly, the delivery of payloads which deliver both ransomware and general disruptive technology such a trojan malware etc
- Educating your front line staff is key – running successful phishing campaigns to educate users on a regular basis second to campaigns on how to identify these type of emails

Access Control

- Protecting your organisation from whom is required and authorized to access your network
  - Role Based Access Control
  - Strong controls within your DMZs
  - Strong Change Management practices (Four eyes checks)
  - IP Whitelisting (Knowing the IP addressing which should be accessing your network)
  - IDS/IPS – Learning about the correct activity within your estate such as Monitoring mode versus preventive mode
- Segregation of duties and admin controls
  - Each department/supporting teams should have the level of RBAC access they require to carry out their duties. However, any elevated access beyond the duties of their roles should not be given. These types of controls limit the exploit opportunities which can be casted upon them or targeted.
  - Appropriate user of Standard AD accounts versus Administrative Accounts (ADM_)

Compensating security controls to your estate

- Controls such as IDS/IPS, Firewall, Security Perimeters
  - Securing your estate with generic Anti Virus (McAfee, Trend, Sophos etc) coupled with Security Controls is not enough in todays area of Disruption.
  - Organisations are moving towards a model of supplementing securing toolsets coupled with security controls.
  - Advanced controls that used to be deployed at the edge of the network are not being embedded
    - Firewall technology such as Intrusion Detection (Monitoring of network activity) and Intrusion Prevention is shifting from the edge of the network (internet link) to being an important barrier between internal systems
    - Preventing suspicious activity from occurring within a network and enforcing ACLs (Access Control Lists) which allow “Only” a nominated list of IP ranges (Subnets and VLANs) access to a network or platform.
  - We often see port security on Switches being activated for a more secure segregation and use of each zone of network.

Deception

- Creating deception within your estate is key
- Always expecting the unexpected
    - it is most important to catch attackers prior to laterally moving between networks and applications and causing disruptive damage.
    - Creation a deception estate or decoy/phantom IT infrastructure on the battlefield is key. Suppliers such as TrapX (an Israeli deception company setup by former members of the IDF) or Attivio are key platforms to allowing your attacker to believe they are truly penetrating your network within all zones (traps should be placed).
    - Not only will you and your SOC learn how the attackers entered your network, but you will also find out how your toolsets and security controls were exploited in addition to all tools run while operating within your estate. Having this type of information (if learning lessons from) can allow you to prevent future attacks and put in place, stronger security controls to protect against this “behaviour” in the future. Afterall, learning an attackers behaviour and activities is key in this cases to mitigation and protect against future Zero Days

Testing

- Vulnerability Scanning
  - Internal (on network) & External (from public)
  - Can be automated with multiple offerings available
- Blue Team/Red Team exercises:
  - Real (skilled) people regularly testing attacks and defences on the environment
  - Always strongly recommended to run.
  - In addition to these exercises, more and more frameworks are being developed. Tiber-EU as an example from ECB for Financial institutes