CHARTA LEARNING · LESSON NOTES

Cyberthreats and Information Security

FRM Part II

1 A story: Monday morning at Larkspur Bank

- An email from the 'CEO' asks for an urgent payment
- A clerk opens a booby-trapped 'invoice'
- By noon, branch screens show a ransom note
- Nobody knows which systems hold customer data
- An IT problem, or a business problem?

IN THE LESSON

- Picture a Monday morning at Larkspur Bank, a mid sized lender.
- An email that seems to come from the chief executive asks the finance team to make an urgent payment to a new supplier.
- Down the corridor, a clerk opens an attachment that looks like an invoice, and it quietly installs malicious software on the laptop.
- By noon, screens across the branches show a ransom note: the files are locked, and the attackers want payment to unlock them.
- Worse, when the board asks which systems hold customer data, nobody can say for sure.
- So here is the question for this lesson.
- Was this an I T problem, or a business problem?
- By the end you will see why it is a risk for the whole firm, owned at the top.

2 What cyber risk is

- Loss from attacks on, or failures of, information systems
- Covers attacks and accidents alike
- Built around three properties: C, I and A
- Losses: money, data, service, fines, reputation
- A risk to the business, not only to the IT department

IN THE LESSON

- Let us define it.
- Cyber risk is the risk of loss from attacks on, or failures of, information systems.
- Notice that the definition covers both.
- A criminal breaking in is cyber risk, but so is a failed system update that takes the payment platform offline for a day.
- The whole subject is built around three properties of information, which we meet next: confidentiality, integrity and availability, often shortened to the C I A triad.
- The losses come in many forms: money stolen or paid out, data lost, services interrupted, fines from regulators, and damage to reputation as customers lose trust.
- That already answers part of our opening question.
- Because the losses land on the business, cyber risk is a risk to the business, and not only to the I T department.

3 Confidentiality, integrity, availability

Every cyber incident damages at least one of three properties

Property	It means
Confidentiality	Only the right people can see the data
Integrity	Data and systems are accurate, unaltered
Availability	Systems work when they are needed

IN THE LESSON

- Here are the three properties.
- Every cyber incident damages at least one of them.
- Confidentiality means that only the right people can see the data.
- When a customer list is stolen, confidentiality is lost.
- Integrity means that data and systems are accurate and have not been altered without authority.
- If an attacker changes the account number on a payment, or a balance in a ledger, integrity is lost, and for a bank that is very serious, because nobody can trust the books.
- Availability means that systems work when they are needed.
- If customers cannot reach online banking for a day, availability is lost.
- Protecting information means protecting all three at once, and an exam question will often ask you to name which property an incident has damaged.

4 Example 1: which property was hit?

Five incidents at Larkspur Bank: which property did each one damage?

Customer files copied out	seen by outsiders	**Confidentiality**
Payment amounts changed	data altered	**Integrity**
Website flooded with traffic	denial of service	**Availability**
Files locked by ransomware	systems unusable	**Availability**
Insider sells a client list	insider misuse	**Confidentiality**

IN THE LESSON

- Let us practise on five incidents at Larkspur.
- First, an attacker copies customer files out of the bank.
- Outsiders can now see the data, so confidentiality is damaged.
- Second, someone changes the amounts on a batch of payments.
- The data has been altered, so integrity is damaged.
- Third, the bank's website is flooded with junk traffic until it stops responding.
- That is a denial of service, and it damages availability.
- Fourth, ransomware locks the files on the branch systems.
- The data is still there but scrambled, so nobody can use it, and availability is the property chiefly damaged.
- Many gangs also steal a copy first, which hits confidentiality too.
- Fifth, an employee sells a list of wealthy clients to a competitor.
- That is insider misuse, and it damages confidentiality.
- The second case, the altered payments, is often the hardest to spot, because nothing looks broken.

5 Common threats, part one

How attackers most often reach a bank

Threat	What happens
Phishing	Fake message tricks staff into a click
Business email compromise	Fake or hijacked email orders a payment
Ransomware	Files locked; ransom demanded to unlock

IN THE LESSON

- Now the threats themselves, starting with the ways attackers most often reach a bank.
- Phishing is a fake message, usually an email, that tricks a member of staff into clicking a link, opening an attachment or typing in a password.
- It is cheap, and it only has to work once.
- Business email compromise is a close cousin.
- A fake email, or a real account that attackers have taken over, orders a payment, often posing as the chief executive or a trusted supplier, just like the urgent payment request in our story.
- Ransomware is malicious software that locks, or encrypts, the victim's files, and the attackers demand a ransom to unlock them.
- For a bank, the lost availability can stop branches and payments, so the pressure to pay is intense.

6 Common threats, part two

Threats that hide inside, or come in through partners

Threat	What happens
Malware	Hidden software spies, steals or damages
Denial of service	Floods of traffic knock a service offline
Insider misuse	Staff abuse the access they were given
Supply chain compromise	Attack arrives via a trusted supplier

IN THE LESSON

- Four more threats complete the list, and some of them hide inside or come through partners.
- Malware is the general name for malicious software, and it can spy on users, steal data or damage systems.
- Ransomware is one kind of malware.
- A denial of service attack floods a website or a network with so much traffic that genuine customers cannot get through, so it attacks availability.
- Insider misuse is when staff, or contractors, abuse the access they were legitimately given, whether for money or out of grievance.
- Firewalls do little here, because the insider is already inside.
- Last, supply chain compromise.
- The attack arrives through a trusted supplier, for example a software update or a service provider that has itself been breached.
- Larkspur did nothing wrong, yet the attack walks in through a door it trusted.

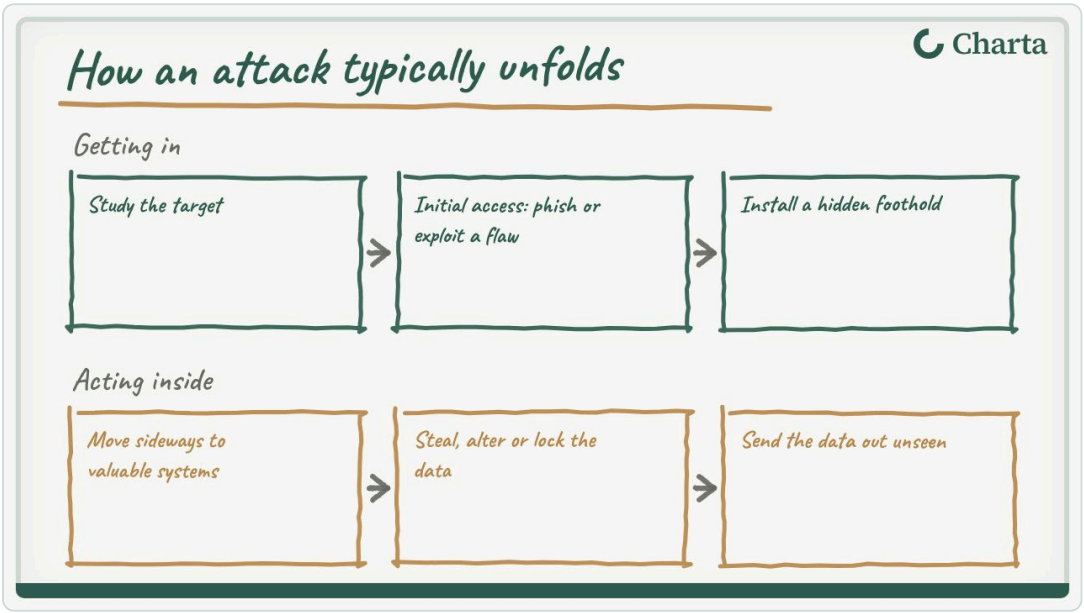
7 Advanced persistent threats

- APT: a slow, well-resourced, targeted campaign
- Gains a foothold and stays hidden, sometimes for months
- Patient: maps the network before acting
- Defence: assume intruders may already be inside
- Hunt for them; do not just guard the door

IN THE LESSON

- Some attackers are in no hurry.
- An advanced persistent threat, shortened to A P T, is a slow, well resourced and targeted campaign.
- Advanced, because the attackers are skilled and well funded.
- Persistent, because they gain a foothold and stay hidden, sometimes for months.
- They are patient.
- They map the network, learn where the valuable data sits, and only then act.
- This changes the defender's mindset.
- If a capable attacker may already be inside, it is not enough to guard the front door.
- The bank must assume that intruders may already be present, and actively hunt for signs of them inside its own systems.
- Keep this idea of assuming a breach in mind, because it returns twice in this lesson, once in good practice and once in the Equifax story.

8 How an attack typically unfolds



IN THE LESSON

- It helps to see an attack as a chain of steps.
- Look at the boxes.
- Getting in comes first.
- The attackers study the target: its staff, its suppliers and its public websites.
- Then they gain initial access, by phishing someone or by exploiting a flaw in software that faces the internet.
- Then they install a hidden foothold, so they can come back.
- Acting inside comes next.
- They move sideways, from the first machine they reach to the systems that matter, such as customer databases.
- They steal, alter or lock the data.
- And if the goal is theft, they send the data out, trying to stay unseen.
- The good news is that every link in the chain is a chance for the defender to break it.
- A control at any one step can stop or expose the whole attack.

9 Cyber risk is an enterprise risk

- An enterprise risk, not only an IT issue
- The board owns it: strategy, appetite, oversight
- Management runs it; IT and security operate controls
- Report in business terms the board understands
- Back to the story: a business problem, owned at the top

IN THE LESSON

- Now to management.
- The first principle is to treat cyber risk as an enterprise risk, not only an I T issue.
- The board owns it.
- It sets the strategy, decides how much cyber risk the bank is willing to accept, which is its risk appetite, and oversees whether the bank stays inside it.
- Senior management runs the programme, and the technology and security teams operate the controls day to day.
- For this to work, reporting must be in business terms the board understands, such as which critical services could stop, for how long, and at what cost, rather than lists of technical alerts.
- Back to our story.
- Larkspur's chaos was not a failure of one laptop.
- It was a business problem, and the answer has to be owned at the top.

10 Prevention in layers

Defence in depth: each layer stops some of what the last one missed

Control	What it does
Patching	Fixes known flaws before attackers use them
Least privilege	Each user gets only the access needed
Segmentation	Walls inside the network limit spread
Encryption	Stolen data is unreadable without the key
Multi-factor authentication	A stolen password alone is not enough

IN THE LESSON

- Good management layers its defences, an idea called defence in depth: each layer stops some of what the last one missed.
- Here are five key prevention layers.
- Patching means installing the fixes that software makers publish for known flaws, before attackers use them.
- Least privilege means each user and system gets only the access it needs for its job, so one stolen account opens few doors.
- Segmentation builds walls inside the network, so an intruder who gets into one part cannot easily reach the rest.
- Encryption scrambles data, so that stolen data is unreadable without the key.
- And multi factor authentication asks for a second proof of identity, such as a code sent to a phone, so a stolen password alone is not enough.
- No single layer is perfect.
- Together they are strong.

11 Example 2: why layers multiply

Larkspur receives 2,000 phishing emails a year. Assume the layers act independently

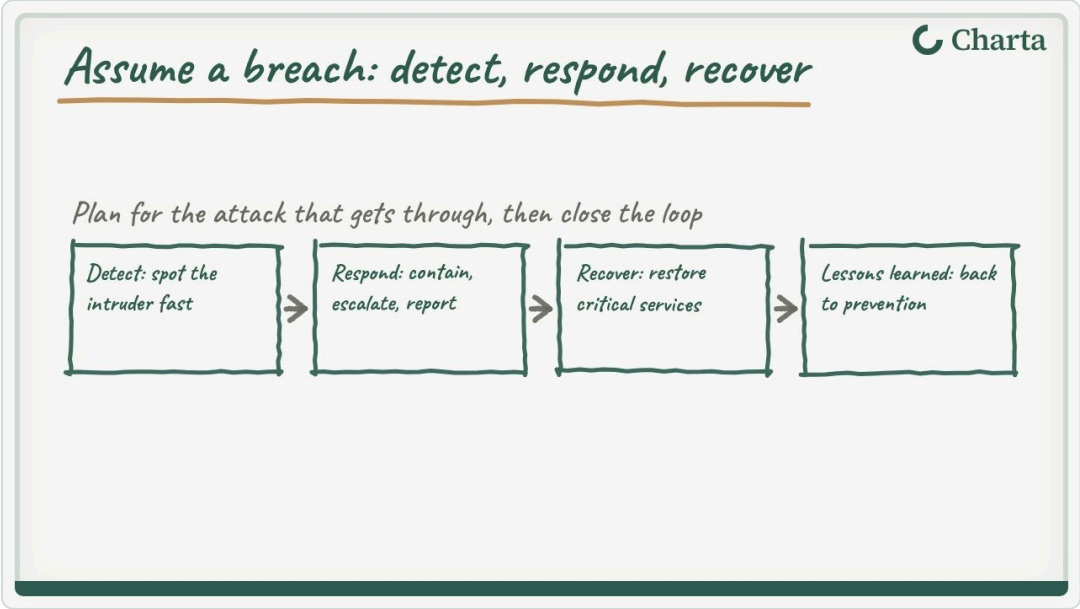
Phishing emails received	a year	**2,000**
Reach inboxes	2,000 × 5%	**100**
Click after training (80% spot it)	100 × 20%	**20**
Taken over, with MFA	20 × 10%	**2**
Taken over, without MFA	20 × 100%	**20**

Layers multiply, but 2 still get in: so plan for a breach

IN THE LESSON

- Let us put numbers on defence in depth.
- Larkspur receives two thousand phishing emails a year, and we assume the layers act independently.
- The email filter blocks ninety five per cent, so five per cent, one hundred emails, reach inboxes.
- Training means eighty per cent of the people who get one spot the fake, so twenty per cent click and enter their password: twenty people.
- Multi factor authentication stops ninety per cent of those, because a password alone is not enough, so two accounts are taken over.
- Without M F A, all twenty would be taken over, ten times as many.
- Two lessons follow.
- Layers multiply, so each extra layer cuts the damage sharply.
- But even three good layers let two attackers in, which is why the bank must also plan for a breach.

12 Assume a breach: detect, respond, recover



IN THE LESSON

- So the second principle is to assume that a breach will eventually happen, and plan for the attack that gets through.
- Look at the boxes.
- Detect means spotting the intruder fast, by monitoring networks, systems and unusual behaviour.
- Every day an intruder goes unseen is another day of damage.
- Respond means containing the attack, for example by cutting off infected machines, escalating to senior management, and reporting to regulators and customers where required.
- Recover means restoring the critical services, such as payments, from clean backups, within a time the business can live with.
- Then comes the last box, the step that closes the loop: the lessons learned from every incident feed back into prevention.
- A bank that is good at all of this may still be attacked, but it suffers far less.

13 Example 3: insurance moves the cost, not the chance

10% yearly chance of a $40m attack. Policy: deductible $5m, limit $25m

Loss if the attack happens		**$40m**
Insurer pays	min(40 − 5, 25)	**$25m**
Larkspur keeps	40 − 25	**$15m**
Chance of attack	unchanged by cover	**10%**
Expected loss kept	10% × 15	**$1.5m**

Before cover: 10% × 40 = $4m expected. Premium is extra

IN THE LESSON

- Many firms buy cyber insurance.
- Here is what it can and cannot do.
- Larkspur estimates a ten per cent chance a year of a ransomware attack costing forty million dollars.
- Its policy has a deductible of five million, the first slice the bank pays itself, and a limit of twenty five million, the most the insurer will pay.
- If the attack happens, the loss is forty million.
- The insurer pays the smaller of forty minus five, which is thirty five, and the limit of twenty five, so it pays twenty five million.
- Larkspur keeps forty minus twenty five, fifteen million: its five million deductible plus the ten million above the limit.
- Now the key row.
- The chance of attack is unchanged by the cover: still ten per cent.
- So the expected loss kept is ten per cent of fifteen, one point five million.
- Before cover it was ten per cent of forty, four million, and the premium is extra.
- Insurance transfers some financial loss, but it does not make an attack less likely.

14 Frameworks that guide the work

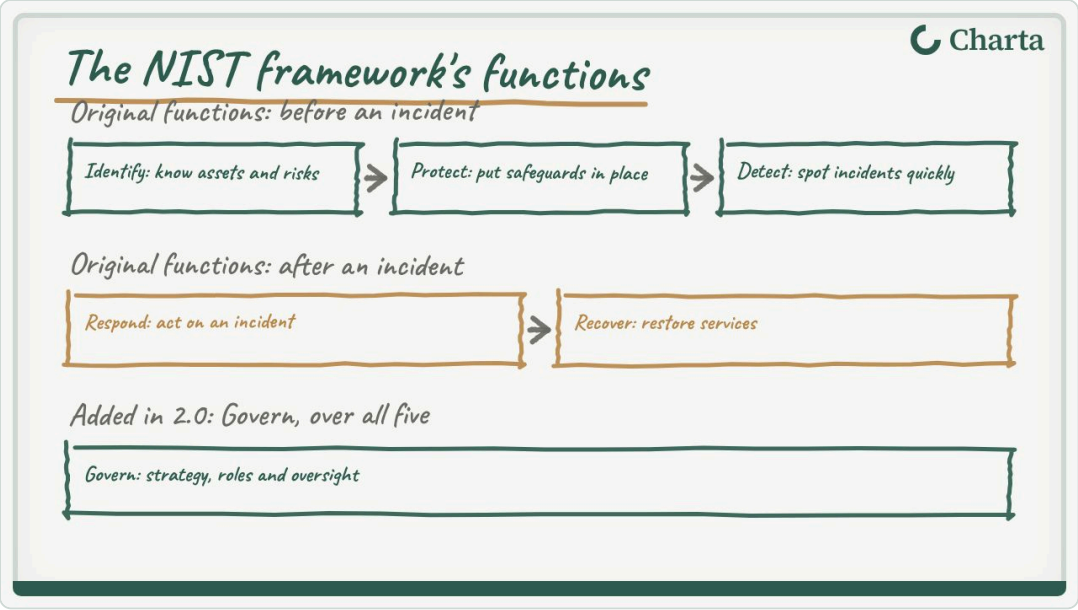
Three widely used frameworks; firms often combine them

Framework	What it gives you
NIST Cybersecurity Framework	Functions to organise a programme
ISO/IEC 27001	A standard for managing info security
COBIT	A framework for governing IT as a whole

IN THE LESSON

- Firms do not invent all this from scratch.
- Three widely used frameworks guide the work, and firms often combine them.
- The N I S T Cybersecurity Framework, from the United States National Institute of Standards and Technology, gives a set of functions to organise a cyber programme around.
- We look at those functions next.
- I S O, I E C twenty seven thousand and one is an international standard for managing information security, through a management system of policies, risk assessment and controls, and an organisation can be certified against it.
- COBIT is a framework for governing and managing information technology as a whole, linking I T to business goals, so it helps with the governance side.
- For the exam, recognise all three, and know the N I S T functions in detail.

15 The NIST framework's functions



IN THE LESSON

- The N I S T framework organises the work into functions.
- Look at the boxes.
- The original five come first, in two rows.
- Before an incident, identify means knowing your assets, your data, your suppliers and your risks, because you cannot protect what you do not know you have.
- Protect means putting safeguards in place, such as the layers we just met.
- Detect means spotting incidents quickly.
- After an incident, respond means acting on an incident: containing it, communicating and reporting.
- Recover means restoring services and learning from what happened.
- The last row is the addition: version two point zero of the framework added a sixth function, govern.
- It covers strategy, roles and responsibilities, and oversight, and it sits over the other five, which matches the idea that cyber risk is owned by the board.
- A question may be built on the original five, so know both versions.

16 Example 4: Larkspur's plan mapped to NIST

Which NIST function does each action in Larkspur's plan belong to?

Build a list of every system	asset inventory	**Identify**
Require MFA for all staff	a second proof of identity	**Protect**
Watch network logs day and night	security monitoring	**Detect**
Run the ransomware playbook	contain and report	**Respond**
Restore from offline backups	services back online	**Recover**

Govern: the board approves strategy and appetite, and oversees it all

IN THE LESSON

- After the Monday attack, Larkspur draws up a plan.
- Let us map each action to a function.
- Building a list of every system the bank owns, an asset inventory, belongs to identify.
- That is the step Larkspur had failed when the board asked where customer data sat.
- Requiring M F A for all staff, a second proof of identity, is protect.
- Watching network logs day and night is security monitoring, which is detect.
- Running the ransomware playbook, a written and rehearsed plan to contain the attack and report it, is respond.
- Restoring systems from offline backups, copies the attackers could not reach, to bring services back online, is recover.
- And above all five sits govern: the board approves the strategy and the appetite and oversees the whole programme.

17 Mistakes to avoid: managing cyber risk

The exam favours layered, tested, board-owned answers

Tempting answer	Better answer
Buy one new security tool	Layered controls, tested regularly
Cyber is an IT matter	An enterprise risk owned by the board
Insurance cuts the risk	Moves some cost; likelihood unchanged
Good prevention is enough	Assume breach: detect, respond, recover
NIST has five functions	Five, plus govern in version 2.0

IN THE LESSON

- Before the case study, here are the traps.
- The exam favours layered, tested, board owned answers.
- The first tempting answer is to buy one new security tool.
- The better answer is layered controls, tested regularly, because any single control will sometimes fail.
- The second is to say cyber is an I T matter.
- Better: it is an enterprise risk owned by the board.
- The third is to say insurance cuts the risk.
- It moves some of the cost, but the likelihood of attack is unchanged.
- The fourth is to think good prevention is enough.
- Better: assume a breach, and be ready to detect, respond and recover.
- The fifth is to say the N I S T framework has five functions.
- That was true of the original, but version two point zero has those five plus govern.

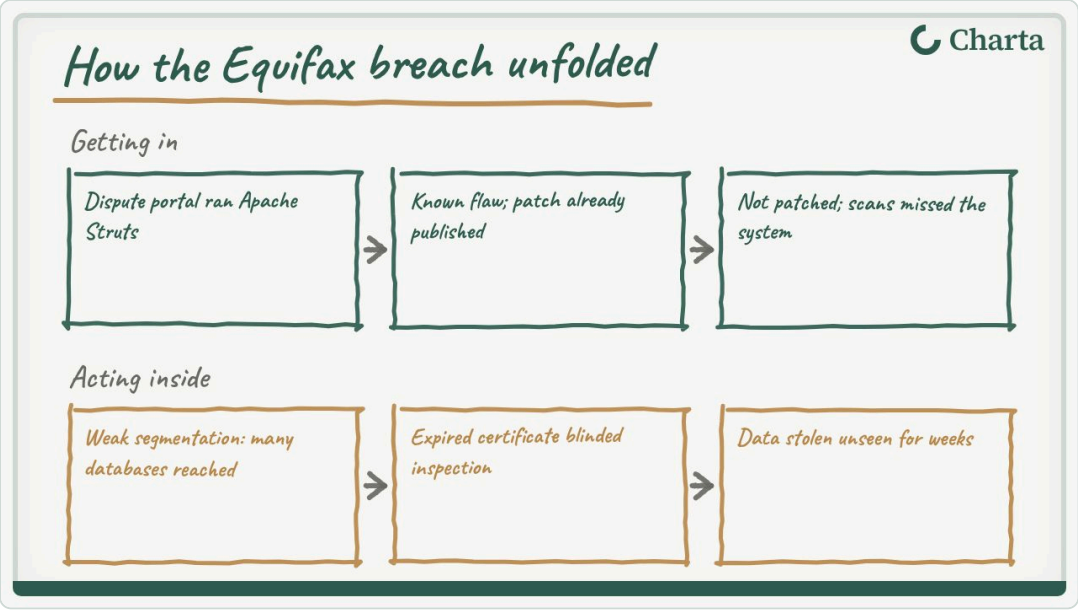
18 The Equifax case: what was at stake

- 2017: breach at Equifax, a major credit bureau
- Personal data of roughly 147 million consumers exposed
- Holds details used to verify identity: hard to reissue
- Cause: a chain of ordinary control failures
- Not an exotic attack: a lesson for every firm

IN THE LESSON

- Now to a real case.
- In two thousand and seventeen, Equifax, a major credit bureau, suffered a breach that exposed the personal data of roughly one hundred and forty seven million consumers.
- A credit bureau, also called a credit reporting agency, collects information about people's borrowing and repayment, and holds the kind of personal details that lenders use to verify who someone is.
- Details like that cannot simply be reissued, the way a bank card can be replaced, so the harm lasts.
- What makes the case so useful for a risk manager is its cause.
- It was not an exotic attack using some unknown weapon.
- It was a chain of ordinary control failures, each of which a well run firm is supposed to prevent.
- That is the lesson for every firm, including Larkspur Bank, and we will trace the chain link by link.

19 How the Equifax breach unfolded



IN THE LESSON

- Here is the chain, using the same two stages as our general attack.
- Look at the boxes.
- Getting in first.
- Equifax ran a public facing portal where consumers could dispute entries on their credit files.
- It was built on Apache Struts, a widely used framework for building web applications.
- Struts had a known flaw, and a patch for that flaw had already been published.
- But the portal was not patched, and the scans that should have found the weakness missed the system.
- Acting inside next.
- Once inside, weak segmentation let the intruders reach many databases.
- An expired certificate on a device that inspected network traffic had left that device blind.
- So the data was stolen and carried out unseen for weeks.
- Each box is an ordinary control that failed, and we take them in turn.

20 Failure one: a known flaw left open

- A patch existed, but nobody made sure it was applied
- Patch ownership failed: no clear owner for the fix
- Asset visibility failed: systems not well tracked
- Vulnerability scanning did not find the system
- Lesson: complete inventory, and verify every patch

IN THE LESSON

- Take the first failure.
- A vulnerability is a weakness in software that an attacker can exploit, and a patch is the fix the software maker publishes.
- Here, a patch existed, but nobody made sure it was applied.
- Why not?
- Two things failed.
- Patch ownership failed: there was no clear owner responsible for making sure this fix reached this system.
- And asset visibility failed: the organisation did not have a good enough view of which systems ran the vulnerable software.
- On top of that, vulnerability scanning, the automated checking that should catch exactly this, did not find the affected system.
- The lesson is to keep a complete asset inventory and to verify every patch, which means checking that the fix is really in place, not just that an instruction was sent.
- Our next example shows why the inventory matters so much.

21 Example 5: a patch rate that flatters

Larkspur lists 950 public-facing systems, 931 patched. A scan finds 50 more of them

Listed systems patched	931 ÷ 950	**98.0%**
Unlisted systems found	none of them patched	**50**
True patch rate	931 ÷ (950 + 50)	**93.1%**
Unpatched systems	(950 − 931) + 50	**69**
Hidden from the list	50 ÷ 69	**72.5%**

IN THE LESSON

- Larkspur reports that its public facing systems are ninety eight per cent patched.
- Its inventory lists nine hundred and fifty systems, and nine hundred and thirty one are patched: nine hundred and thirty one over nine hundred and fifty is ninety eight per cent.
- Then a discovery scan finds fifty public facing systems that were not on the list, and none of them is patched.
- The true patch rate is nine hundred and thirty one over nine hundred and fifty plus fifty, which is one thousand, so ninety three point one per cent.
- The unpatched systems are nine hundred and fifty minus nine hundred and thirty one, nineteen, on the list, plus fifty off it, sixty nine in all.
- Fifty over sixty nine is seventy two point five per cent: that share of the unpatched systems was hidden from the list.
- The metric looked healthy because its denominator was wrong.
- Systems missing from the list are the ones nobody patches, which is the asset visibility failure behind Equifax.

22 Failure two: weak segmentation

- Segmentation: internal walls between parts of a network
- At Equifax, weak walls let intruders reach many databases
- One entry point became access to far more data
- Good design: sensitive data in separate zones
- Lesson: segment networks to limit the blast radius

IN THE LESSON

- The second failure came after the attackers got in.
- Segmentation means building internal walls between parts of a network, so that a system facing the public cannot freely talk to the databases behind it.
- At Equifax, segmentation was weak, and the intruders were able to reach many databases.
- So one entry point, a single dispute portal, became access to far more data than that portal itself needed.
- Good design keeps sensitive data in separate zones, with tightly controlled paths between them, and gives the public facing system only the narrow access its job requires, which is least privilege applied to the network.
- The lesson is to segment networks to limit the blast radius, meaning how far the damage spreads from the point of entry.
- In the attack chain, segmentation is the control that breaks the move sideways.

23 Failure three: the blind inspection device

- Data leaving the network is mostly encrypted
- An inspection device decrypts and checks it
- Its certificate had expired, so it saw nothing
- Outbound data theft went unseen for weeks
- Lesson: monitor encrypted traffic; keep tools working

IN THE LESSON

- The third failure is the subtlest.
- Most traffic leaving a modern network is encrypted, scrambled so that outsiders cannot read it.
- That protects customers, but it also hides what attackers send out.
- So firms use an inspection device that decrypts outgoing traffic, checks it for anything suspicious, and passes it on.
- To do that, the device relies on a digital certificate, an electronic credential that has an expiry date.
- At Equifax, the certificate on such a device had expired, so it could not inspect the traffic, and in effect it saw nothing.
- The outbound data theft went unseen for weeks.
- The control existed on paper, but it was not working.
- The lesson is to monitor encrypted traffic, and to keep the monitoring tools themselves working, which includes tracking simple things like certificate expiry dates.

24 Example 6: what detection time costs

Attackers copy 25,000 records a day from Larkspur until someone notices

Records copied per day	made-up rate	**25,000**
Caught in 3 days	25,000 × 3	**75,000**
Blind for 60 days	25,000 × 60	**1,500,000**
How many times worse	60 ÷ 3	**20 times**

Exposure grows with time unseen: fix the monitoring, not just the door

IN THE LESSON

- Here is why the blind device mattered so much.
- Suppose attackers inside Larkspur copy twenty five thousand records a day until someone notices.
- That is a made up rate.
- If working monitoring catches the outbound traffic in three days, twenty five thousand times three is seventy five thousand records lost.
- Serious, but contained.
- If instead the inspection device is blind and the theft runs for sixty days, twenty five thousand times sixty is one million five hundred thousand records.
- That is sixty over three, twenty times worse, from the same break in.
- Exposure grows with the time the attacker is unseen.
- This is why we assume a breach.
- Detection is not a nice extra after prevention: it decides whether an incident is small or a disaster, so fix the monitoring, not just the door.

25 A chain of ordinary failures

Each Equifax failure, and the control that should have stopped it

What failed	Control that should have worked
Unpatched known flaw	Verified patching, clear owner
System not in view	Complete asset inventory
Scans missed it	Scanning that covers every asset
Weak segmentation	Separate zones, least privilege
Expired inspection certificate	Monitoring of encrypted traffic

IN THE LESSON

- Let us line up the chain.
- Each Equifax failure sits next to the control that should have stopped it.
- The unpatched known flaw calls for verified patching, with a clear owner for every fix.
- The system not being in view calls for a complete asset inventory.
- The scans missing it calls for scanning that covers every asset, which again depends on the inventory.
- Weak segmentation calls for separate zones and least privilege inside the network.
- And the expired inspection certificate calls for monitoring of encrypted traffic that actually works.
- Notice that every one of these controls is ordinary and well known.
- None needed new technology.
- Any one of them working might have stopped the attack or cut it short.
- Large losses usually come from several ordinary failures lining up, and the defence is to make each layer really work.

26 Lessons from Equifax

- Keep a complete asset inventory
- Verify that patches are really applied
- Monitor encrypted traffic, and keep the tools working
- Segment networks to limit how far intruders get
- Clear accountability, with senior oversight

IN THE LESSON

- Here are the lessons in one place.
- First, keep a complete asset inventory, because the systems you do not know about are the ones nobody patches or watches.
- Second, verify that patches are really applied, and do not assume that publishing a fix or sending an instruction is the same as fixing the flaw.
- Third, monitor encrypted traffic, and keep the monitoring tools themselves working.
- Fourth, segment networks to limit how far intruders get once inside.
- Fifth, and underlying the rest, assign clear accountability, with senior oversight.
- Behind the patching failure was an ownership gap: no one clearly owned the fix.
- This is where the case meets the first half of the lesson.
- Board owned, layered and tested controls are exactly what this chain of failures was missing.

27 Mistakes to avoid: reading the case

Common wrong conclusions from the Equifax story

Wrong conclusion	Better conclusion
An unstoppable, exotic attack	Ordinary controls failed in a chain
Patch published, so it was fixed	Only a verified patch counts
Encrypted traffic is safe traffic	Encryption can hide data theft
One team made one mistake	Accountability and oversight failed

IN THE LESSON

- Exam questions on this case often tempt you with wrong conclusions.
- The first is that it was an unstoppable, exotic attack.
- The better conclusion is that ordinary controls failed in a chain.
- The second is that because the patch was published, the problem was fixed.
- Only a patch that has been verified on every affected system counts.
- The third is that encrypted traffic is safe traffic.
- Encryption protects data from outsiders, but it can also hide data theft, which is why it must be inspected.
- The fourth is that one team made one mistake.
- The better conclusion is that accountability and oversight failed, so the fix is about governance and not only about technology.
- If an answer option offers a single technical fix as the whole lesson, it is probably the trap.

28 Recap

- Cyber risk threatens confidentiality, integrity, availability
- Phishing, BEC, ransomware, insiders, supply chain
- Board-owned layers; assume breach; insurance moves cost
- Frameworks: NIST (5 + govern), ISO 27001, COBIT
- Equifax: inventory, patch, scan, segmentation, monitoring

IN THE LESSON

- Let us recap.
- Cyber risk is the risk of loss from attacks on, or failures of, information systems, and it threatens confidentiality, integrity and availability.
- The threats include phishing, business email compromise, ransomware, insiders and supply chain compromise, among others.
- Good management is board owned, layered, and assumes a breach will happen, so detection, response and recovery matter as much as prevention, and insurance moves some cost but not the chance of attack.
- The frameworks are N I S T, with its five functions plus govern, I S O twenty seven thousand and one, and COBIT.
- And Equifax shows a chain of ordinary failures, not an exotic attack: inventory, patching, scanning, segmentation and monitoring all fell short.

29 Try three quick questions

1. 800 phishing emails. Filter blocks 90%, 25% of the rest click, MFA stops 95%. Takeovers?
   Answer: 80 get through, 20 click, 5% × 20 = 1 account.
2. Attack loss $30m. Deductible $2m, limit $20m. Insurer pays? Chance of attack?
   Answer: min(28, 20) = $20m; bank keeps $10m. Chance unchanged.
3. Equifax: which failure let the data theft go unseen for weeks?
   Answer: Expired certificate on the inspection device: monitor encrypted traffic.

IN THE LESSON

- Now try three quick questions.
- Pause the video, think, then listen to the answers.
- Question one.
- A bank receives eight hundred phishing emails.
- The filter blocks ninety per cent, a quarter of the emails that get through are clicked, and multi factor authentication stops ninety five per cent of those.
- How many accounts are taken over?
- Eighty emails get through, twenty are clicked, and five per cent of twenty is one account.
- Question two.
- An attack costs thirty million dollars.
- The policy has a deductible of two million and a limit of twenty million.
- What does the insurer pay, and does the chance of attack change?
- Thirty minus two is twenty eight, capped at twenty, so the insurer pays twenty million and the bank keeps ten.
- The chance is unchanged.
- Question three.
- In the Equifax case, which failure let the data theft go unseen for weeks?
- The expired certificate on the traffic inspection device, so monitor encrypted traffic.