CHARTA LEARNING · LESSON NOTES

Case Study: Third-Party Risk

FRM Part II

1 A story: the outage that was not Kestrel's fault

- Kestrel outsources card payments to Corvane Payments
- Corvane's systems fail for three hours one afternoon
- Customers cannot pay, and they blame Kestrel
- The regulator asks Kestrel, not Corvane, to explain
- The service moved out; the accountability did not

IN THE LESSON

- Kestrel Bank is a mid sized lender.
- Three years ago it outsourced its card payment processing to a specialist firm, Corvane Payments, which is bigger, cheaper and better at it than Kestrel could be on its own.
- Then one busy afternoon, Corvane's systems fail for three hours.
- Kestrel's customers stand at checkouts with cards that do not work.
- Who do they blame?
- Not Corvane, a name most of them have never heard.
- They blame Kestrel, and they call Kestrel's helpline.
- The next morning the regulator writes, and the letter goes to Kestrel, not to Corvane, asking what happened and what Kestrel will do about it.
- That is the heart of this lesson.
- The service moved out of the building, but the accountability did not move with it.

2 Why firms use third parties

- Third party: an outside firm supplying a product or service
- Outsourcing: it performs work the firm could do itself
- Buy capability: skills and technology the firm lacks
- Buy scale: capacity that grows with the business
- Buy cost savings: the provider shares its fixed costs

IN THE LESSON

- Let us start with two definitions.
- A third party is any outside firm that supplies a product or a service to the bank.
- Outsourcing is the special case where the third party performs an activity the bank could otherwise do itself, such as processing payments or running a call centre.
- Why do it?
- There are three reasons.
- First, to buy capability: skills and technology the firm does not have and could not easily build, such as a specialist payments engine.
- Second, to buy scale: capacity that can grow with the business without the firm building it all in advance.
- Third, to buy cost savings, because the provider spreads its fixed costs over many clients.
- Kestrel gained all three from Corvane.
- None of these benefits is in doubt.
- The question is what comes with them.

3 Accountability does not transfer

- A contract moves the work, not the responsibility
- The firm answers to customers for the outsourced activity
- The firm answers to its regulators for it too
- The board and senior management still own the risk
- Exam point: responsibility cannot be outsourced

IN THE LESSON

- The first thing that comes with outsourcing is a rule you must never forget.
- A contract moves the work, not the responsibility.
- The firm stays answerable to its customers for the outsourced activity, exactly as if it still did the work itself.
- Kestrel's customers have an account with Kestrel, and their complaint is with Kestrel.
- The firm also stays answerable to its regulators.
- A supervisor will not accept the excuse that the failure happened at a supplier.
- Inside the firm, this means the board and senior management still own the risk of every outsourced service, and must be able to show they oversee it.
- So the exam point of this module can be said in four words.
- Responsibility cannot be outsourced.
- Everything in the framework we build follows from that one idea.

4 Four new risks a third party adds

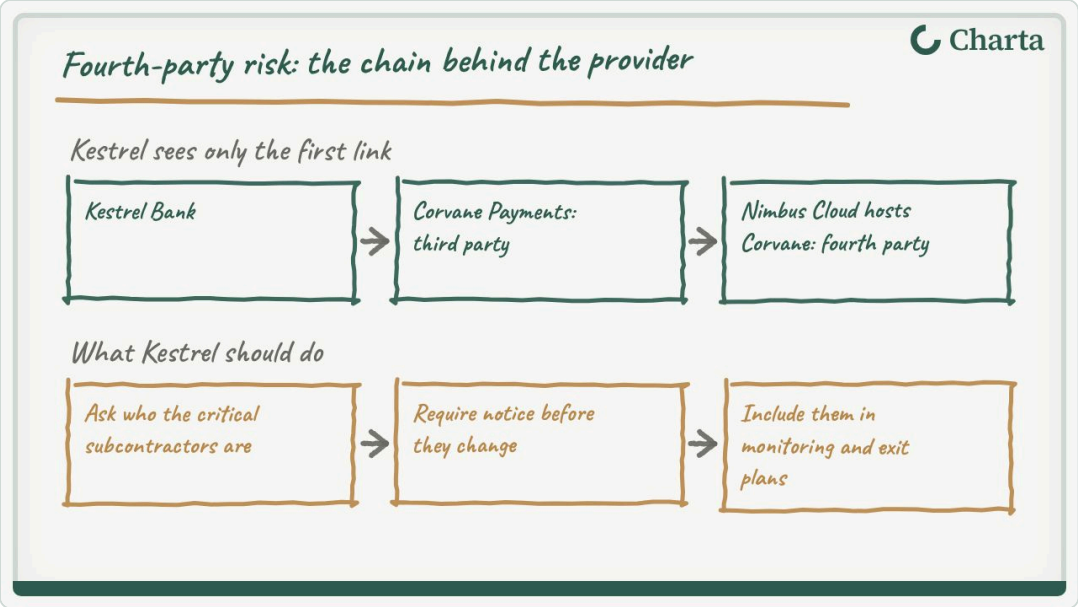
Using a provider adds risks the firm did not have when it did the work itself

New risk	What it means for Kestrel
Loss of control and visibility	Cannot see inside or fix Corvane
Dependence on the provider	Its people, systems and controls
Fourth-party risk	Corvane's own subcontractors
Concentration risk	Many functions or firms, one provider

IN THE LESSON

- Outsourcing also adds risks that Kestrel did not have when it did the work itself.
- The table names four.
- The first is loss of direct control and visibility.
- When Corvane's systems fail, Kestrel cannot see inside them, and cannot fix them.
- It can only wait and ask.
- The second is dependence on the provider.
- Kestrel now relies on Corvane's people, Corvane's systems and Corvane's controls, none of which it chose or manages day to day.
- The third is fourth party risk.
- A fourth party is the provider's own subcontractor, so the risk comes from firms Kestrel has no contract with at all.
- The fourth is concentration risk.
- It arises when many functions of one firm rely on the same provider, or when many firms across the industry do.
- Then one failure hits everything at once.

5 Fourth-party risk: the chain behind the provider



IN THE LESSON

- Let us look more closely at fourth party risk, because it is easy to miss.
- Look at the top row.
- Kestrel Bank has a contract with Corvane Payments, its third party.
- But Corvane does not run its own data centres.
- It rents computing power from a cloud provider, Nimbus Cloud, which is Kestrel's fourth party.
- Kestrel sees only the first link of the chain, yet a failure at Nimbus would stop Kestrel's card payments just as surely as a failure at Corvane.
- What should Kestrel do?
- The bottom row gives three steps.
- First, ask Corvane who its critical subcontractors are.
- Second, require notice before Corvane changes them.
- Third, include those fourth parties in Kestrel's own monitoring and exit plans.
- You cannot manage a risk you cannot see, so the first job is to make the chain visible.

6 Example 1: measuring concentration

Kestrel maps its 12 critical services to the providers that run them

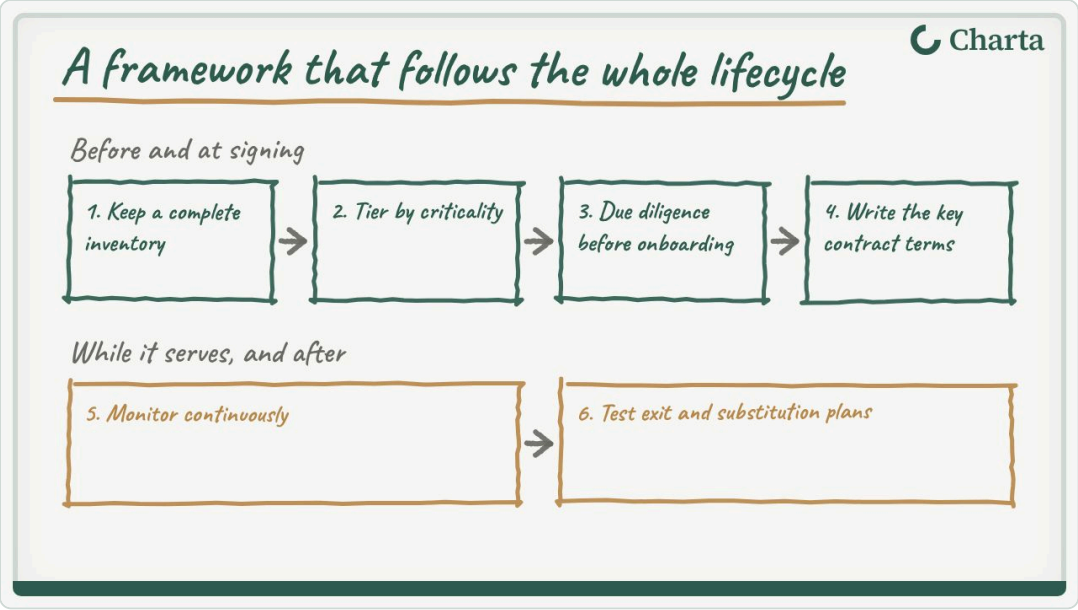
Critical services	mapped this year	**12**
Run on Nimbus Cloud	2 direct, 5 via providers	**7**
Share on one provider	7 ÷ 12	**58.3%**
Board limit per provider	one third of 12	**4**
Excess over the limit	7 − 4	**3 services**

Industry layer: many banks may rely on Nimbus too

IN THE LESSON

- Here is concentration risk in numbers.
- This year Kestrel maps its twelve critical services to the firms that actually run them.
- Seven of the twelve turn out to run on Nimbus Cloud.
- Only two use Nimbus directly.
- The other five use it through providers like Corvane, so the dependence was hidden one link down the chain.
- Seven over twelve is fifty eight point three per cent of Kestrel's critical services resting on one provider.
- Kestrel's board has set a limit of one third of critical services on any one provider, which is four of the twelve.
- So Kestrel is three services over its own limit.
- And there is a second layer.
- If many other banks also rely on Nimbus, then a Nimbus failure is not one bank's problem but the whole industry's, all at the same moment.

7 A framework that follows the whole lifecycle



IN THE LESSON

- Now to the framework that works well.
- Its defining feature is that it follows the whole life of the relationship, not just the start.
- Look at the top row, before and at signing.
- Step one is to keep a complete inventory of providers.
- Step two is to tier them by how critical they are.
- Step three is due diligence before onboarding, meaning the investigation of the provider before it is allowed to start work.
- Step four, before signing, is to write the key terms into the contract.
- Now the bottom row, while the provider serves and after.
- Step five is to monitor the provider continuously.
- And step six is to test the exit and substitution plans, meaning the plans to leave the provider, or to replace it, without stopping the service.
- We take each step in turn, using Kestrel.

8 Step one: a complete inventory

- List every provider, not only the big technology contracts
- Record the service, the data it touches, its access
- Record its key subcontractors: the fourth parties
- Map which critical services depend on it
- No inventory: no tiering, no monitoring, no exit plan

IN THE LESSON

- Step one sounds dull, but everything else depends on it.
- A complete inventory lists every provider, not only the big technology contracts that went through the purchasing department.
- When Kestrel built its first inventory, it found software subscriptions bought by business teams on their own budgets, which nobody in risk knew existed.
- For each provider, the inventory records the service it delivers, the data it touches and the access it has to Kestrel's systems.
- It also records the provider's key subcontractors, the fourth parties we just met.
- And it maps which critical services depend on each provider, which is exactly how Kestrel found its hidden reliance on Nimbus.
- Without an inventory, there is nothing to tier, nothing to monitor, and no exit plan, because you cannot plan to leave a provider you do not know you have.

9 Step two: tier by criticality, not contract value

Tier on how critical the service and the data are, not on what the contract costs

Tier	When it applies	Oversight
1: critical	Critical service, sensitive data or wide access	Deepest, most frequent
2: important	Material service, or limited data or access	Regular review
3: low	Easily replaced, no data access	Light touch

IN THE LESSON

- Step two is tiering, which means sorting providers into groups that get different amounts of oversight.
- The key rule is in the grey line.
- Tier on how critical the service and the data are, not on what the contract costs.
- The table shows a simple three tier scheme.
- Tier one, critical, covers a provider whose service is critical, or who holds sensitive data or wide access.
- It gets the deepest and most frequent oversight.
- Tier two, important, covers a material service, or a provider with limited data or access, and gets regular review.
- Tier three, low, covers a provider that is easily replaced and has no access to data, and gets a light touch.
- Why not tier by contract value?
- Because a cheap contract can carry enormous risk, as our first case study will show.

10 Example 2: tiering by criticality, not spend

Score = criticality (1-3) × data/access sensitivity (1-3). Tier 1: 6+, Tier 2: 3-5, Tier 3: 1-2

Office supplies firm	$900k: 1 × 1	**1: Tier 3**
Payroll processor	$150k: 2 × 3	**6: Tier 1**
Heating contractor	$40k: 1 × 3	**3: Tier 2**
Corvane Payments	$2.0m: 3 × 3	**9: Tier 1**

By spend, office supplies ranks 2nd; by risk it is last

IN THE LESSON

- Let us tier four of Kestrel's providers.
- Each gets a score: how critical the service is, from one to three, times how sensitive its data and access are, from one to three.
- A score of six or more is tier one.
- Three to five is tier two, and one or two is tier three.
- The office supplies firm has a contract of nine hundred thousand dollars, but scores one times one, which is one, so tier three.
- The payroll processor costs only one hundred and fifty thousand dollars, but it holds every employee's personal and bank details.
- It scores two times three, six, so tier one.
- The heating contractor costs forty thousand dollars, but has remote access to building systems on Kestrel's network.
- It scores one times three, three, so tier two.
- Corvane, at two million dollars, scores three times three, nine, tier one.
- Ranked by spend, office supplies would come second.
- By risk it comes last.

11 Step three: due diligence before onboarding

- Financial strength: can the provider keep serving?
- Controls and security: how is our data protected?
- Resilience: backups, recovery times, tested plans
- Subcontractors: who are the fourth parties?
- Depth scales with the tier

IN THE LESSON

- Step three is due diligence before onboarding, the investigation Kestrel makes before a provider is allowed to start.
- It asks a series of questions.
- Financial strength: is the provider sound enough to keep serving for the life of the contract?
- Controls and security: how will Kestrel's data and systems be protected, and who at the provider can reach them?
- Resilience: what backups does the provider keep, how fast can it recover, and does it test its own plans?
- Subcontractors: who are the fourth parties, and what do they do?
- Finally, the depth of all this scales with the tier.
- A tier one provider like Corvane gets a full review with site visits and evidence.
- A tier three office supplies firm gets a short questionnaire.
- Proportion is the point, because time spent on the low tier is time taken from the critical one.

12 Step four: write the key terms into the contract

Rights not written in before signing are very hard to win afterwards

Contract term	What it gives Kestrel
Audit rights	Can inspect and audit the provider
Service levels	Measurable standards, such as uptime
Incident notification	Told quickly when things go wrong
Exit terms	Help and time to leave in order

IN THE LESSON

- Step four is the contract.
- The grey line gives the reason it matters so much.
- Rights not written in before signing are very hard to win afterwards, because once the provider is running a critical service, the firm has little leverage.
- The table shows four terms a sound contract contains.
- Audit rights let Kestrel inspect and audit the provider, rather than simply take its word.
- Service levels set measurable standards, such as how many minutes of downtime are allowed each month.
- Incident notification requires the provider to tell Kestrel quickly when something goes wrong, so Kestrel can warn customers and its regulator.
- And exit terms give Kestrel the help and the time to leave in an orderly way, including the return of its data.
- Notice that every one of these protects Kestrel's own ability to answer for the service.

13 Example 3: did Corvane meet its service level?

Contract: 99.9% availability per 30-day month; notify incidents within 1 hour

Minutes in a 30-day month	30 × 24 × 60	**43,200**
Downtime allowed	0.1% × 43,200	**43.2 min**
Actual outage	3 hours	**180 min**
Excess over the limit	180 − 43.2	**136.8 min**
Notice given after	required within 1 hour	**2 hours: late**

Service credits do not repay customers or reputation

IN THE LESSON

- Back to the afternoon of the outage.
- Corvane's contract promises ninety nine point nine per cent availability in each thirty day month, and notice of any incident within one hour.
- A thirty day month has thirty times twenty four times sixty minutes, which is forty three thousand two hundred minutes.
- One tenth of one per cent of that is the downtime allowed: forty three point two minutes.
- The actual outage lasted three hours, one hundred and eighty minutes.
- So Corvane exceeded its limit by one hundred and thirty six point eight minutes.
- And it told Kestrel after two hours, not within the one hour required, so the notice was late too.
- Kestrel can claim service credits, meaning a fee reduction.
- But those credits do not repay Kestrel's customers, or its reputation.

14 Step five: monitor continuously

- Track service levels, incidents and complaints monthly
- Watch financial health, ownership and key staff
- Watch for new subcontractors and new uses of data
- Re-tier when the service or the risk changes
- Review Tier 1 providers most often and most deeply

IN THE LESSON

- Step five is continuous monitoring, and it is where many firms fall short.
- A provider that passed due diligence three years ago may be a different firm today.
- So Kestrel tracks service levels, incidents and customer complaints every month.
- It watches the provider's financial health, any change of ownership, and the loss of key staff.
- It watches for new subcontractors and for new uses of Kestrel's data.
- When the service or the risk changes, it re tiers the provider, moving it up or down.
- And it reviews tier one providers most often and most deeply.
- Had Kestrel been monitoring closely, a rising number of small Corvane incidents in the months before the outage might have warned it.
- Monitoring turns a one off check into a running picture of the risk.

15 Example 4: testing the exit plan

Kestrel tests leaving Corvane. The contract gives 12 months' notice

Choose and contract a new firm	estimated	**4 months**
Migrate data and test	estimated	**8 months**
Run both in parallel	estimated	**3 months**
Total time to exit	4 + 8 + 3	**15 months**
Gap versus notice period	15 − 12	**3 months short**

Fix: longer transition support, or a warm alternative

IN THE LESSON

- Step six is to test exit and substitution plans.
- An exit plan says how to leave a provider in an orderly way.
- A substitution plan says how to replace it, with another provider or by bringing the work back in house.
- Kestrel tests its exit from Corvane on paper, step by step.
- Corvane's contract gives twelve months' notice.
- Choosing and contracting a new provider is estimated at four months.
- Migrating the data and testing the new system takes eight months.
- Running both in parallel, to make sure nothing is lost, takes three more.
- The total time to exit is fifteen months, so the plan is three months short of the notice period.
- Without the test, Kestrel would have learned that in a crisis.
- The fix is to write longer transition support into the contract, or to keep a warm alternative ready.

16 Mistakes to avoid in the framework

- Treating onboarding diligence as the whole job
- Tiering by contract value instead of criticality
- Thinking the contract transfers the responsibility
- Ignoring fourth parties and concentration
- Writing an exit plan but never testing it

IN THE LESSON

- Let us gather the mistakes.
- The usual one is treating onboarding diligence as the whole job, as if a provider that was safe on the first day stays safe forever.
- The second is tiering by contract value instead of by criticality, which puts a cheap provider with sensitive data at the bottom of the pile.
- The third is thinking the contract transfers the responsibility.
- It does not, as Kestrel's letter from the regulator showed.
- The fourth is ignoring fourth parties and concentration, which hides risks one link down the chain, as with Nimbus.
- And the fifth is writing an exit plan but never testing it, which leaves a plan that fails exactly when it is needed.
- The exam point to remember is this.
- Risk management follows the whole lifecycle, and responsibility cannot be outsourced.

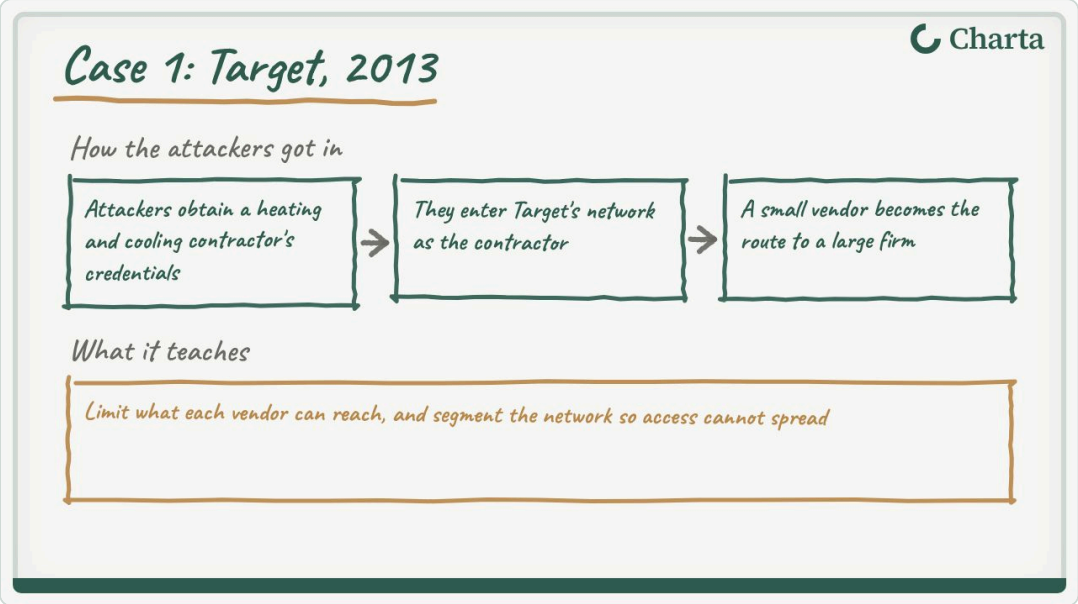
17 The case studies: one pattern, different triggers

- Target, 2013: a contractor's credentials let attackers in
- SolarWinds, 2020: a trusted update was corrupted
- CrowdStrike, 2024: a faulty update crashed machines
- Different triggers, the same pattern
- A vendor's failure became the customer's own incident

IN THE LESSON

- Now to the case studies.
- We look at three real third party failures.
- Their triggers differ, but they share a pattern.
- In twenty thirteen, at the retailer Target, attackers got in through the credentials of a contractor.
- In twenty twenty, at SolarWinds, a trusted vendor's software update was itself corrupted.
- And in July twenty twenty four, a faulty update from CrowdStrike crashed machines around the world, with no attacker involved at all.
- So the triggers are different: stolen credentials, a corrupted update and a simple error.
- But the pattern is the same.
- In every case, a vendor's failure became the customer's own operational incident.
- The customers, not the vendors, faced their own clients and their own disruption.
- We take each case in turn, and then ask what Kestrel should learn.

18 Case 1: Target, 2013



IN THE LESSON

- The first case is the Target breach of twenty thirteen.
- Look at the top row, how the attackers got in.
- First, the attackers obtained the credentials of a heating and cooling contractor, a small firm that had network access to do its job for Target.
- Second, they used those credentials to enter Target's network, posing as the contractor.
- Third, the result: a small vendor with network access became the route into a large firm.
- The attackers did not have to break down Target's front door.
- They walked in through a side door that a supplier held the key to.
- Now the bottom row, what it teaches.
- First, limit what each vendor can reach to what it truly needs.
- Second, segment the network, meaning divide it into separate zones, so that access to one zone cannot spread to the others.

19 Why a small vendor mattered so much

- The contractor was small, and its contract was small
- But its network access made it a door into the firm
- Tiering by spend would rank it near the bottom
- Access, not size, sets the risk
- Lesson: least privilege inside a segmented network

IN THE LESSON

- Why does this case matter so much for the framework?
- Because the contractor was small, and its contract was small.
- But its network access made it a door into the firm.
- Think back to the tiering slide.
- A scheme that tiered providers by spend would rank a heating contractor near the very bottom, with a light touch questionnaire and little monitoring.
- So the first lesson is that access, not size, sets the risk.
- Any vendor that can log in to the firm's network deserves to be treated as a potential route for an attacker.
- The practical rule is called least privilege.
- Each vendor gets only the access its job needs, and nothing more, inside a segmented network.
- Then a stolen password opens one small room, not the whole building.

20 Example 5: Kestrel reviews vendor access

Kestrel finds 40 vendors with wide remote access to its network

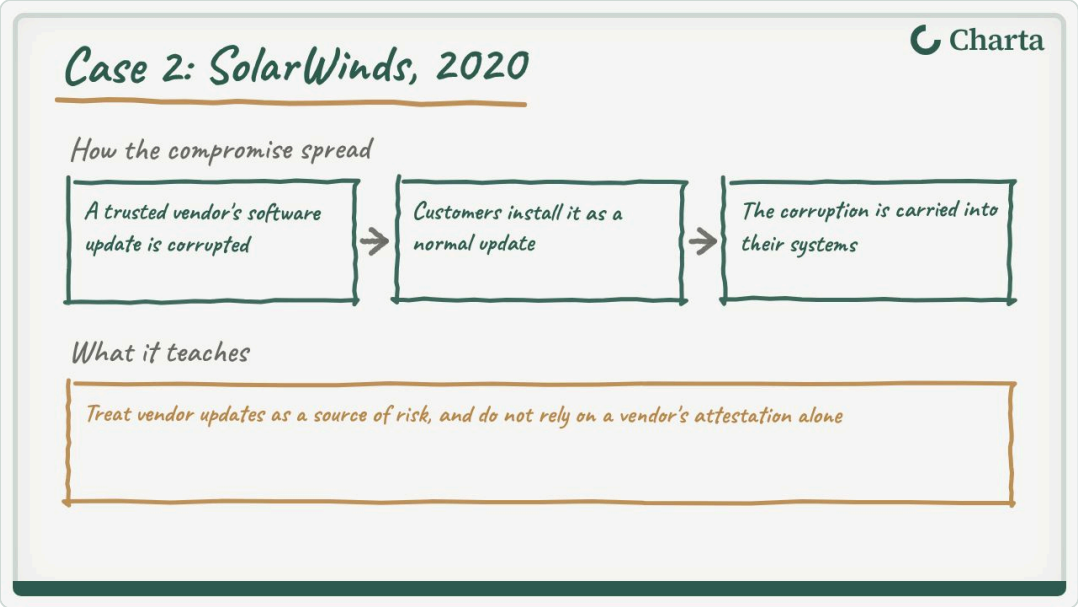
Vendors with wide remote access	found in the review	**40**
Need no access at all	removed	**10**
Need one system only	restricted and segmented	**24**
Need wider access	Tier 1, sessions monitored	**6**
Vendors with wide access	(40 − 6) ÷ 40	**85% fewer**

30 can still log in; 24 reach one segmented system

IN THE LESSON

- Kestrel takes the lesson home.
- It reviews every vendor that can reach its network remotely, and finds forty, all with wide access.
- Ten of them need no access at all any more.
- Some finished their projects years ago, but nobody removed their accounts.
- Those are removed.
- Twenty four need access to one system only, such as the heating contractor, who needs the building controls and nothing else.
- Their access is restricted to that one system, and that system is segmented from the rest of the network.
- Only six need wider access, and they are all tier one providers, with their sessions monitored.
- So vendors with wide access fall from forty to six.
- Forty minus six is thirty four, and thirty four over forty is an eighty five per cent cut in wide access.
- Thirty vendors can still log in, but twenty four of them reach only one segmented system.

21 Case 2: SolarWinds, 2020



IN THE LESSON

- The second case is the SolarWinds compromise of twenty twenty, and here the route was different.
- Look at the top row, how the compromise spread.
- First, a trusted vendor's software update was itself corrupted, before it ever left the vendor.
- Second, its customers installed it as a normal update, because that is what customers of a trusted vendor do.
- Third, the corruption was carried into their own systems, through the very channel meant to keep those systems up to date.
- No customer was careless in the usual sense.
- They did what good practice told them to do, and kept their software current.
- The bottom row draws two lessons.
- First, treat vendor software updates as a source of risk, not as automatically safe.
- Second, do not rely on a vendor's attestation alone.

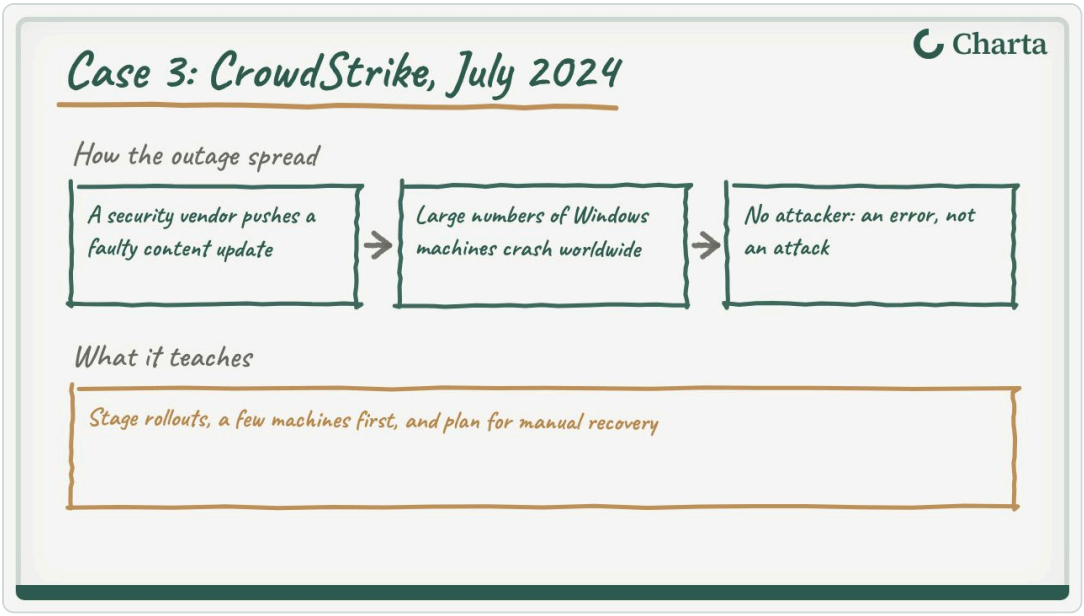
22 Why trust was the weak point

- Trusted vendors' updates are installed routinely
- An attestation may not catch a corrupted update
- Limit what vendor software can reach and change
- Watch how it behaves after each update
- Trust the vendor, but verify and contain

IN THE LESSON

- Why was trust the weak point?
- Updates from a trusted vendor are installed routinely, often automatically, so they pass straight through the firm's defences.
- An attestation is a vendor's formal statement, often backed by an auditor's report, that its controls are working.
- It is useful evidence, but it may not catch a problem like a corrupted update, and it is no substitute for the firm's own defences.
- So what can a firm do?
- First, limit what vendor software can reach and change, so a bad update cannot touch everything.
- Second, watch how the software behaves after each update, and investigate anything unusual.
- The summary is a phrase worth remembering.
- Trust the vendor, but verify and contain.
- Kestrel now treats its software vendors' updates as changes to be checked, not as gifts.

23 Case 3: CrowdStrike, July 2024



IN THE LESSON

- The third case is the CrowdStrike outage of July twenty twenty four, and it is different again.
- Look at the top row, how the outage spread.
- First, a security vendor pushed a faulty content update to its customers' machines.
- Second, large numbers of Windows machines crashed, all around the world, at almost the same time.
- Third, and this is the key point, there was no attacker.
- This was an error, not an attack.
- A product bought to protect firms became the cause of their outage.
- That matters for the exam, because it shows that third party risk is not only cyber attack.
- A simple mistake by a trusted vendor can do the same damage.
- The bottom row shows what this case teaches.
- First, stage rollouts, meaning a few machines first.
- Second, plan for manual recovery.

24 Example 6: why staged rollouts and manual recovery matter

Kestrel has 8,000 machines. A faulty update needs 10 minutes of hands-on repair each

All at once: machines down	every machine	**8,000**
Repair work: 8,000 × 10 min	80,000 min ÷ 60	**≈ 1,333 hours**
With 40 technicians	1,333 ÷ 40	**33.3 hours**
Staged: first wave only	1% of 8,000	**80**
With 40 technicians	80 × 10 ÷ 40	**20 min**

A manual recovery plan says who fixes what, in what order

IN THE LESSON

- Here is why those two lessons matter, using Kestrel's own numbers.
- Kestrel has eight thousand machines.
- Suppose a faulty update leaves each one needing ten minutes of hands on repair.
- If the update reaches every machine at once, all eight thousand are down.
- The repair work is eight thousand times ten minutes, which is eighty thousand minutes, or about one thousand three hundred and thirty three hours.
- With forty technicians, that is about thirty three point three hours of non stop work.
- Now suppose the rollout is staged, and the first wave goes to one per cent of machines, eighty of them.
- The fault shows up there, and the rollout stops.
- Repairing eighty machines with forty technicians takes eighty times ten, divided by forty, just twenty minutes.
- And a manual recovery plan says in advance who fixes what, and in what order.

25 The three cases side by side

Different triggers, one pattern: the vendor's failure became the customer's incident

Case	What failed	Main lesson
Target, 2013	Contractor credentials used	Limit and segment access
SolarWinds, 2020	Trusted update corrupted	Treat updates as a risk
CrowdStrike, 2024	Faulty update, no attacker	Stage rollouts, manual recovery

IN THE LESSON

- Let us put the three cases side by side.
- The grey line repeats the pattern: different triggers, one pattern, as the vendor's failure became the customer's incident.
- In the Target case of twenty thirteen, what failed was that a contractor's credentials were used to get in, and the main lesson is to limit and segment vendor access.
- In the SolarWinds case of twenty twenty, a trusted update was corrupted, and the main lesson is to treat vendor updates as a source of risk.
- In the CrowdStrike case of twenty twenty four, a faulty update crashed machines with no attacker, and the main lesson is to stage rollouts and plan for manual recovery.
- Notice that only the first two involved an attacker at all.
- A question that assumes every vendor incident is a cyber attack has already gone wrong.

26 The lessons, put together

- Limit and segment vendor access
- Treat vendor software updates as a source of risk
- Stage rollouts and plan for manual recovery
- Do not rely on attestation or contract alone
- Build your own resilience

IN THE LESSON

- Put together, the case studies give five lessons, and you should be able to list them.
- First, limit and segment vendor access, so that a stolen credential opens one room, not the building.
- Second, treat vendor software updates as a source of risk, even from the most trusted vendor.
- Third, stage rollouts and plan for manual recovery, so that a bad update hits a few machines, and the firm knows how to bring them back by hand.
- Fourth, do not rely on a vendor's attestation or on the contract alone.
- Both are useful, but neither keeps the firm running on the day the vendor fails.
- And fifth, the lesson that sums up the others: build your own resilience.
- The firm must be able to keep serving its customers whatever happens at the vendor.

27 Where each lesson fits in Kestrel's framework

Each case lesson strengthens a step of the lifecycle framework

Lesson	Where it fits in the framework
Limit and segment access	Tiering and monitoring
Treat updates as a risk	Monitoring and change control
Stage rollouts, manual recovery	Contract and own recovery plans
Not attestation alone	Audit rights and own testing

IN THE LESSON

- Each case lesson strengthens a step of the lifecycle framework we built earlier, and the table shows where.
- Limiting and segmenting access belongs in tiering, because access raises the tier, and in monitoring, because access must be reviewed as it changes.
- Treating updates as a risk belongs in monitoring and in change control, which is the firm's process for checking any change before it is put into use.
- Staged rollouts and manual recovery belong in the contract, where the firm can ask for a say over timing, and in the firm's own continuity and recovery plans.
- Not relying on attestation alone belongs in audit rights and the firm's own testing.
- So the case studies do not need a new framework.
- They show what happens when one step of the old one is treated as a formality.

28 Exam traps in the case studies

- Trap: only attacks cause vendor incidents (CrowdStrike)
- Trap: small contracts mean small risk (Target)
- Trap: a trusted vendor's update is safe (SolarWinds)
- Trap: the contract or attestation protects the firm
- Exam point: a vendor failure is your own incident

IN THE LESSON

- Finally, the exam traps.
- The first trap is to think that only attacks cause vendor incidents.
- CrowdStrike is the counter example, an error with no attacker.
- The second trap is to think that small contracts mean small risk.
- Target is the counter example, where a small contractor was the way in.
- The third trap is to think that a trusted vendor's update is safe.
- SolarWinds is the counter example, where the update itself was the weapon.
- The fourth trap is to think that the contract or an attestation protects the firm.
- They help, but they do not keep the firm's services running.
- And so to the exam point that ties the cases together.
- A vendor failure becomes your own operational incident, so you must build your own resilience.

29 Try three quick questions

1. Contract: 99.5% availability over a 30-day month. Downtime allowed?
   Answer: 0.5% × 43,200 = 216 minutes = 3.6 hours.
2. Cleaning firm $1m, no data or access; payroll firm $200k, all staff data. Higher tier?
   Answer: The payroll firm: tier by criticality and data, not cost.
3. A vendor's faulty update crashes your machines; no attacker. Two lessons?
   Answer: Stage rollouts, and plan for manual recovery.

IN THE LESSON

- Now try three quick questions.
- Pause the video, think, then listen to the answers.
- Question one.
- A contract promises ninety nine point five per cent availability over a thirty day month.
- How much downtime is allowed?
- The allowance is half of one per cent of forty three thousand two hundred minutes, which is two hundred and sixteen minutes, or three point six hours.
- Question two.
- A cleaning firm costs one million dollars a year and has no data or system access.
- A payroll firm costs two hundred thousand dollars and holds all staff data.
- Which belongs in the higher tier?
- The payroll firm, because tiering follows criticality and data, not contract value.
- Question three.
- A vendor's faulty update crashes your machines, and there is no attacker.
- Name two lessons.
- Stage rollouts, and plan for manual recovery.