Charta | LESSON NOTES

Digital Resilience and Financial Stability

FRM Part II

1 A story: Merrow's bad year

- March: ransomware locks Merrow's payment servers
- June: a faulty update at cloud provider Velnet
- Online banking stops at Merrow and two rivals
- Board: were both cyber? How does it hit the money?
- And can it threaten the whole system?

IN THE LESSON

- Meet Merrow Bank, a mid sized lender.
- In March, a criminal gang slips ransomware into its network, and the servers that handle customer payments are locked.
- In June, nobody attacks anyone.
- A cloud provider called Velnet pushes out a faulty software update, and online banking stops for a day, not just at Merrow but at two rival banks that use the same provider.
- Both events cost money and both made the news.
- The board asks three questions.
- Were these both cyber events?
- How could a technology fault become a funding or capital problem?
- And if several banks fail at once, is the whole system at risk?
- This lesson answers all three.

2 What cyber risk is

- Cyber risk: loss from malicious, intentional acts
- Against information systems: someone means harm
- Criminals, hostile states, activists or insiders
- Some texts use 'cyber' loosely for any IT failure
- Here: cyber means intent

IN THE LESSON

- Start with cyber risk.
- Cyber risk is the risk of loss from malicious, intentional acts against information systems.
- Someone means to do harm.
- That someone may be a criminal gang after money, a hostile state, an activist, or a person inside the firm.
- The typical forms are ransomware, data theft, denial of service attacks, account takeover and fraud through stolen credentials, and misuse by insiders.
- You may meet texts that use the word cyber loosely, for any failure of information systems.
- In this reading the line is sharper: cyber means intent.
- That is why the March attack on Merrow is a cyber event, and the June update, a mistake with no attacker, is not.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

3 The main forms of attack

Attack	What happens
Ransomware	Files locked; payment demanded to unlock
Data theft	Customer or firm data copied out
Denial of service	Flood of traffic knocks a service offline
Account takeover	Stolen credentials used to move money
Insider misuse	Staff abuse the access they were given

IN THE LESSON

- Here are the main forms of attack in turn.
- Ransomware encrypts a firm's files and systems, and the attacker demands a payment to unlock them, as at Merrow in March.
- Data theft copies customer or firm data out of the network, to sell it or use it for fraud.
- A denial of service attack floods a website or service with traffic until real customers cannot get through.
- Account takeover uses stolen passwords or other credentials to get into a customer's account and move money out, which is fraud through compromised credentials.
- Insider misuse is an employee or contractor who abuses the access they were given, for example to steal data or alter accounts.

4 ICT risk is wider

- Any failure, misuse or compromise of ICT
- Accidental outages; faulty software changes
- Legacy systems; poor data quality
- Weak governance of technology
- Failure of third-party or cloud providers

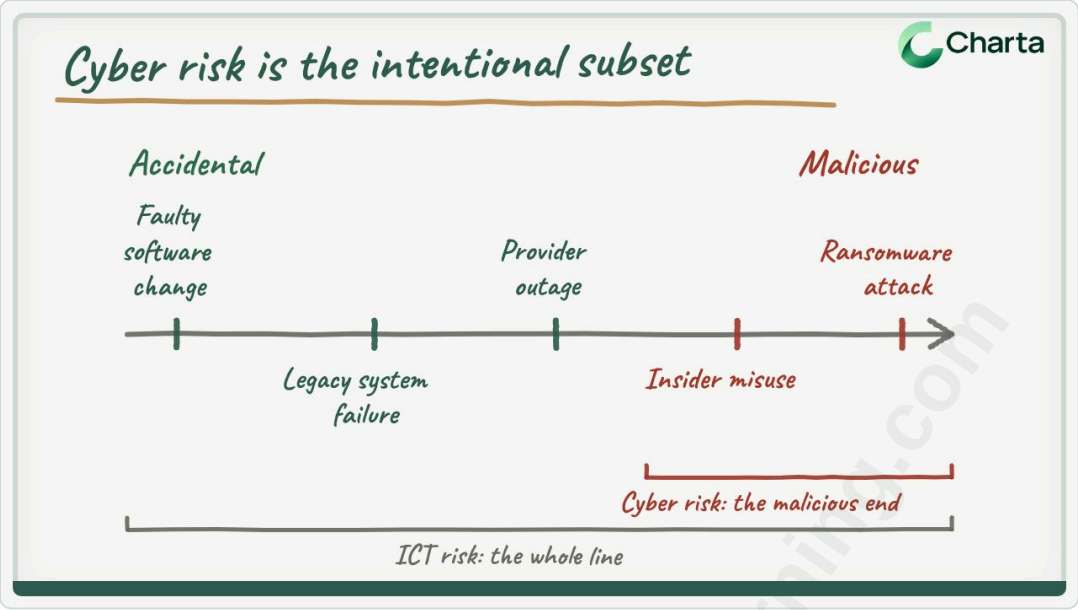
IN THE LESSON

- I C T risk is wider.
- It is the risk of loss from any failure, misuse or compromise of information and communication technology, whether anyone intended it or not.
- So besides attacks, it covers accidental outages, such as a power failure in a data centre.
- It covers faulty software changes, like Velnet's update.
- It covers legacy systems, old technology that is hard to maintain and fragile when changed.
- It covers poor data quality, where the numbers a bank relies on are wrong or incomplete.
- It covers weak governance of technology, such as unclear ownership of systems.
- And it covers the failure of third party or cloud providers that a bank depends on.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

5 Cyber risk is the intentional subset



IN THE LESSON

- Put the two ideas on one line, from accidental on the left to malicious on the right.
- At the left is a faulty software change, an honest mistake.
- Next is a legacy system failure, old technology that breaks.
- Then a provider outage, such as Velnet's day offline, again with no attacker.
- Moving right, we reach insider misuse, where someone inside chooses to do harm.
- At the far right is a ransomware attack by an outside gang.
- The upper bracket, over the malicious end only, is cyber risk.
- The lower bracket, across the whole line, is I C T risk: every one of these events belongs to it.
- So cyber risk is the intentional subset of I C T risk, not another name for it.

6 Confidentiality, integrity, availability

Property	Means	Breached when
Confidentiality	Data not exposed	Data leaked or stolen
Integrity	Data not altered	Data changed or corrupted
Availability	Services usable when needed	A system is down

IN THE LESSON

- How do we describe the damage?
- Usually by three properties of information and systems.
- Confidentiality means data are not exposed to people who should not see them.
- It is breached when customer details leak or are stolen.
- Integrity means data are not altered without authority, so the balances and records a bank holds are correct.
- It is breached when data are changed, by an attacker or by a faulty program.
- Availability means services are usable when needed.
- It is breached when a system is down, as when Merrow's payment servers were locked, or Velnet's update stopped online banking.
- One incident can hit more than one property at the same time.

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

7 Example 1: sorting Merrow's incidents

Merrow's incidents this year: malicious or not, and which property was hit?

Event	Malicious?	Type	Property hit
Ransomware locks payment servers	Yes	Cyber	Availability
Customer data copied and sold	Yes	Cyber	Confidentiality
Faulty update corrupts balances	No	ICT only	Integrity
Velnet outage stops online banking	No	ICT only	Availability
Clerk alters data for a friend	Yes	Cyber	Integrity

IN THE LESSON

- Here is Merrow's incident list for the year.
- For each event, ask two questions: was it malicious, and which property did it hit?
- The ransomware that locked the payment servers was malicious, so it is cyber, and it hit availability.
- Customer data copied and sold was malicious too, so cyber, and it hit confidentiality.
- A faulty update that corrupted account balances was a mistake, so it is I C T risk only, and it hit integrity.
- The Velnet outage was also a mistake, I C T only, and it hit availability.
- Finally, a clerk who altered account data to help a friend acted on purpose, so that is cyber, through insider misuse, and it hit integrity.

8 Why financial firms are exposed

- Business is digital: money is entries in systems
- Tightly connected through payment and settlement
- Many rely on the same few vendors
- Money and data make them attractive targets
- Exam point: ICT risk is more than cyber attacks

IN THE LESSON

- Why are financial institutions so exposed to these risks?
- First, their business is digital.
- Money itself is mostly entries in computer systems, and almost every service, from payments to trading, runs on technology.
- Second, they are tightly connected.
- Banks pay and settle with each other all day through shared payment and settlement systems, so one firm's problem quickly reaches its counterparties.
- Third, many of them rely on the same few vendors, for cloud computing, core banking software and networks, so one supplier's fault can hit many firms at once.
- And money and data make them attractive targets.
- Hence the exam point: do not equate I C T risk with cyber attacks.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

9 Example 2: the cyber-only mistake

Merrow's ICT losses for the year, $m. Its risk report shows only the cyber line

Malicious attacks: cyber	ransomware, fraud	**$12m**
Faulty software changes	accidental	**$18m**
Cloud provider outage	third party, accidental	**$25m**
Legacy systems, poor data	accidental	**$5m**
All ICT losses	12 + 18 + 25 + 5	**$60m**

Cyber-only report: 12 ÷ 60 = 20% of the loss

IN THE LESSON

- Now a classic mistake.
- Merrow's risk report shows only cyber losses.
- Here are its I C T losses for the year in full.
- Malicious attacks cost twelve million dollars.
- Faulty software changes cost eighteen million.
- The cloud provider outage cost twenty five million.
- Legacy systems and poor data cost five million.
- All I C T losses together are twelve plus eighteen plus twenty five plus five, sixty million dollars.
- The cyber only report captures twelve of those sixty, which is just twenty per cent.
- Four fifths of the technology loss, and the largest single item, the provider outage, never reach the board.
- That is what equating I C T risk with cyber attacks costs.

10 From an IT event to a financial one

- An incident starts as an operational event
- It moves into financial risk through channels
- Often several channels at once
- Liquidity and funding can suffer within hours
- Treat it as a financial event from the start

IN THE LESSON

- Now the second question: how does a technology incident become a financial problem?
- A cyber or I C T incident is first an operational event.
- Something stops working, or data are stolen or wrong.
- But it does not stay there.
- It moves into the classic financial risks through several channels, and it can reach many of them at once.
- Liquidity and funding can suffer within hours.
- Credit and market risk can follow, and so can a hit to capital.
- So treat a serious incident as a possible financial event from the start, not only as a job for the technology team.

11 Five channels into financial risk

Channel	How an incident feeds it
Liquidity	Payment outage traps intraday balances
Funding	Lost confidence: deposits and funding leave
Credit	Disrupted borrowers struggle to repay
Market	Bad or missing data distorts prices
Capital	Direct costs and fines cut capital

IN THE LESSON

- Here are the channels one by one.
- Liquidity: a payment outage can trap intraday balances, money that should arrive during the day but is stuck, so the bank cannot use it to meet its own payments.
- Funding: a loss of confidence can make depositors withdraw and lenders withhold funding.
- Credit: when borrowers are disrupted, by an attack on them or on a supplier they rely on, they may struggle to repay, so credit quality weakens.
- Market: corrupted or unavailable data distorts prices and trading, because traders cannot see or trust the numbers.
- Capital: the direct costs of the incident, and any fines, reduce the bank's capital.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

12 Example 3: trapped intraday liquidity

Ransomware stops Merrow booking incoming payments for a day. Figures in $bn

Payments Merrow must make	by the end of the day	**$3.0bn**
Normal sources	2.0 cash + 1.2 incoming	**$3.2bn**
Incoming trapped by the outage	cannot be booked	**– $1.2bn**
Sources left	3.2 − 1.2	**$2.0bn**
Shortfall to borrow	3.0 − 2.0	**$1.0bn**

IN THE LESSON

- In March, the ransomware also stops Merrow from booking the payments it receives.
- Here is its position for the day, in billions of dollars.
- Merrow must make three billion dollars of payments by the end of the day.
- Normally it would use two billion of cash at the central bank plus one point two billion of incoming payments, so three point two billion of sources.
- But the outage traps the incoming one point two billion.
- Sources left are three point two minus one point two, two billion.
- The shortfall is three minus two, one billion dollars, which Merrow must borrow at short notice, on the very day the market has heard it was attacked.
- An operational event has become liquidity stress.

13 Example 4: capital versus confidence

Stress attack: $40m cost plus $20m fine. Capital $3,000m, risk-weighted assets $25,000m

Direct costs and fine	40 + 20	**$60m**
Capital after the loss	3,000 − 60	**$2,940m**
Capital ratio: 12% before	2,940 ÷ 25,000	**11.76%**
Deposits withdrawn	5% × $40bn	**$2,000m**
Withdrawals ÷ direct loss	2,000 ÷ 60	**about 33 times**

IN THE LESSON

- Now compare two other channels, using a stress case, an attack worse than anything in Merrow's log.
- It costs forty million dollars for recovery, experts and compensation, plus a twenty million dollar fine.
- Merrow's capital is three thousand million dollars, against twenty five thousand million of risk weighted assets.
- The direct costs and fine are forty plus twenty, sixty million.
- Capital after the loss is three thousand minus sixty, two thousand nine hundred and forty million.
- The capital ratio was twelve per cent before.
- Now it is two thousand nine hundred and forty divided by twenty five thousand, eleven point seven six per cent.
- That is a small dent.
- But news of the attack frightens large depositors.
- Deposits withdrawn are five per cent of forty billion dollars, two thousand million, or two billion dollars.
- The withdrawals are about thirty three times the direct loss.
- Capital cannot pay out withdrawals, only cash can, so the confidence channel can dwarf the capital channel.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

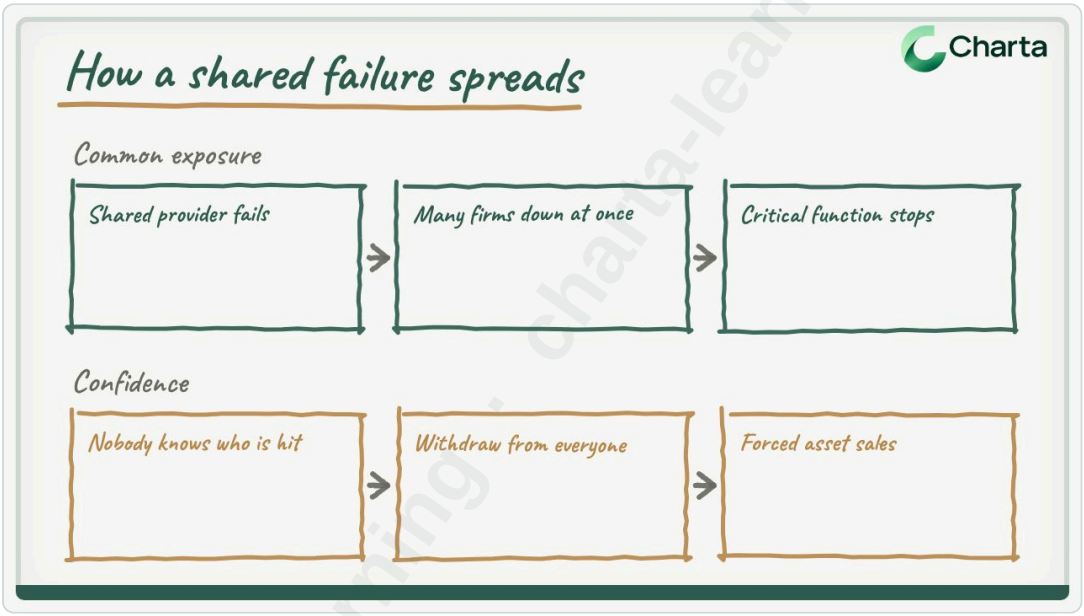
14 When an incident becomes systemic

- Systemic: the system stops paying, lending, settling
- A critical function with no quick substitute
- Many firms share a vendor, software or network
- Amplified by interconnection
- And by information asymmetry: who is affected?

IN THE LESSON

- Systemic risk is the risk that the financial system as a whole stops doing its job, of paying, lending and settling, with harm to the wider economy.
- An incident becomes systemic in two main ways.
- First, when it impairs a critical function that cannot be quickly substituted, such as a large payment system or a central counterparty, because nobody else can step in by tomorrow.
- Second, when many firms share the same vendor, software or network, so their failures happen at the same time.
- Two features amplify both.
- Interconnection carries the problem from firm to firm, and information asymmetry, where outsiders cannot tell who is affected, spreads fear to firms that were never hit.

15 How a shared failure spreads

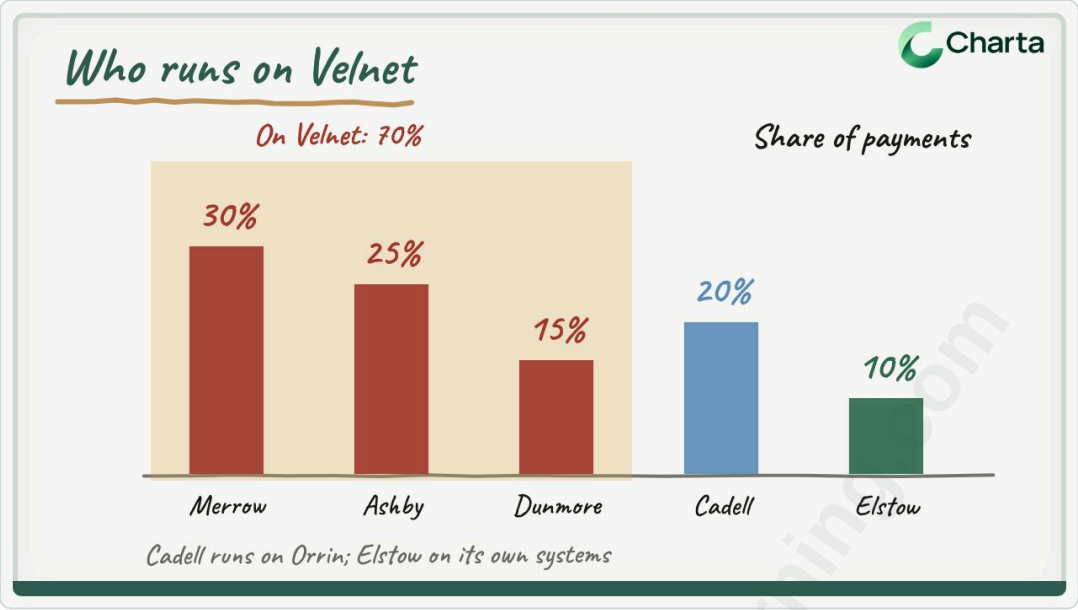


IN THE LESSON

- Here is the mechanism in two rows.
- The first row is common exposure.
- A shared provider fails.
- Many firms go down at once, because they all run on it.
- And a critical function stops, because the firms that would normally take up the slack are down as well.
- The second row is confidence.
- Nobody knows who is hit, since firms do not publish the details of their systems and the first reports are confused.
- So lenders and depositors withdraw from everyone, not only from the firms affected, which is the safe choice for each of them.
- That can force asset sales, as firms sell securities quickly to raise cash, pushing prices down for all holders.

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

16 Who runs on Velnet



IN THE LESSON

- Here is the market Merrow operates in.
- The bars show each bank's share of the market's daily retail payments, and every bar starts from zero.
- Merrow handles thirty per cent, Ashby twenty five, and Dunmore fifteen.
- The shaded band marks the banks that run their payment services on Velnet: those three together carry seventy per cent of the market.
- Next, Cadell handles twenty per cent.
- Elstow handles ten per cent.
- No single bank here is dominant.
- But one provider sits under seventy per cent of the market's payments, and that is the concentration a supervisor should worry about.
- The note says why the other two differ: Cadell runs on a different provider, Orrin, and Elstow on its own systems.

17 Example 5: the size mistake

A: an imagined $300m fraud at Merrow alone. B: a fresh Velnet outage at three banks

A: loss at Merrow alone	payments keep running	**$300m**
B: direct loss, Velnet clients	3 banks × $5m	**$15m**
B: payments stopped	30 + 25 + 15	**70%**
Larger direct loss	300 ÷ 15	**A, 20 times**
The systemic event	common exposure, no substitute	**B**

IN THE LESSON

- A classic mistake is to judge systemic risk by the size of the direct loss.
- Compare two imagined events.
- A is a three hundred million dollar fraud at Merrow alone.
- B is a fresh Velnet outage at three banks.
- In event A, the loss falls on Merrow alone, and its payments keep running; if they stopped, customers could switch to other banks.
- The loss is three hundred million dollars.
- In event B, the direct loss to Velnet's clients is three banks times five million, fifteen million in all.
- But in B the payments stopped are thirty plus twenty five plus fifteen, seventy per cent of the market at once.
- Which direct loss is larger?
- Three hundred divided by fifteen: A, by twenty times.
- Yet the systemic event, through common exposure and no quick substitute, is B.

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

18 The exam point on systemic risk

- Starts operational; reaches all financial risks
- Confidence can dwarf the direct cost
- Systemic: critical function, or shared vendor
- Spread by connectedness and not knowing who is hit
- Exam point: common exposure, not loss size

IN THE LESSON

- So how should you judge the interaction between cyber risk and financial risk?
- Every incident starts as an operational event, but it reaches liquidity, funding, credit, market prices and capital, and the confidence channel can be far larger than the direct cost, as Example four showed.
- It becomes systemic when it stops a critical function with no quick substitute, or when a shared vendor makes failures simultaneous.
- Interconnection and the fog of not knowing who is affected then spread it.
- The exam point: systemic risk comes from common exposure, connectedness and confidence, not from the size of one firm's direct loss.

19 Macroprudential: the system, not the firm

- Microprudential: the safety of one firm
- Macroprudential: the stability of the whole system
- Each firm careful, the system still fragile
- Shared choices impose costs on all: an externality
- Tools make firms and providers count that cost

IN THE LESSON

- Now the third question: what can policy do?
- Microprudential supervision looks after the safety of each firm on its own.
- Macroprudential policy aims at the stability of the whole system.
- For cyber and I C T risk, the system view matters, because each bank can be careful and the system still fragile.
- Merrow, Ashby and Dunmore each chose Velnet for good reasons, but none of them counted the cost of all choosing the same provider.
- That cost falls on everyone, which economists call an externality.
- Macroprudential tools try to make firms and providers take account of it.
- The toolkit has two halves, and we take each in a table.

20 The toolkit, part one

Tool	Aim	Main obstacle
Cyber stress tests	Find common weak points	Scarce loss data
Capital, liquidity add-ons	Absorb losses, outflows	Cannot restore a service
Incident reporting, sharing	Early warning for all	Reputation, liability fears
Threat-led penetration tests	Attack real systems	The test can disrupt

IN THE LESSON

- Here is the first half of the toolkit, with the main obstacle to each.
- System wide cyber stress tests and scenario exercises ask many firms to work through the same severe scenario, to find common weak points.
- Their obstacle is that loss data are scarce, so the scenarios are hard to calibrate.
- Capital and liquidity buffers or add-ons give firms more room to absorb losses and outflows.
- But capital absorbs losses; it does not restore a stopped service.
- Mandatory incident reporting and information sharing give authorities and peers an early warning, but firms fear damage to their reputation and legal liability.
- Threat-led penetration testing attacks a firm's real systems as a genuine attacker would, and the test itself can cause disruption.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

21 The toolkit, part two

Tool	Aim	Main obstacle
Oversight of critical providers	Limits and exit plans	Outside the perimeter
Crisis playbooks	A coordinated response	Many authorities agree
Recovery and resolution	Keep functions running	Few substitutes
Insurance and backstops	Transfer the loss	Correlation, moral hazard

IN THE LESSON

- Here is the second half.
- Direct oversight of critical third party providers lets authorities examine the providers themselves, and set concentration limits and require exit plans.
- The obstacle is that providers sit outside the regulatory perimeter, the boundary of what regulators can supervise, and they often operate across borders.
- Coordinated crisis playbooks set out in advance who does what in a system wide incident, but they need many authorities and countries to agree and practise together.
- Recovery and resolution planning keeps critical functions running if a firm fails, yet substitutes for critical services may be few.
- Risk transfer and backstop arrangements, such as insurance or a public backstop, are limited by correlated losses and moral hazard.

22 Stress tests and buffers in practice

- Same severe scenario for every bank
- Authority adds up the answers: where do failures cluster?
- Exercises: banks, providers, authorities together
- Liquidity buffers help with trapped balances
- Capital add-ons: scarce loss data, weak calibration

IN THE LESSON

- Look closer at the first tools.
- A system wide cyber stress test gives every bank the same scenario, say a major payment system or cloud provider down for two days, and asks how it would cope.
- The authority adds up the answers to see where failures would cluster.
- Scenario exercises do the same thing around a table, with banks, providers and authorities together.
- Liquidity buffers do help with trapped balances, as Merrow's one billion dollar shortfall showed.
- Capital add-ons are harder.
- Because severe cyber losses are rare and firms report few of them, the data needed to set an add-on are scarce, so any number is weakly calibrated, as the next example shows.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

23 Example 6: calibrating a capital add-on

Supervisor sizes a cyber add-on for Merrow. Risk-weighted assets $25,000m

Low estimate of severe loss	vendor model	**$100m**
High estimate	scenario panel	**$600m**
Add-on, low	100 ÷ 25,000	**0.4%**
Add-on, high	600 ÷ 25,000	**2.4%**
Range: high ÷ low	600 ÷ 100	**6 times**

Capital absorbs the loss; it does not restart payments

IN THE LESSON

- The supervisor wants a cyber capital add-on for Merrow, sized to a severe but plausible loss.
- Its risk weighted assets are twenty five thousand million dollars.
- Two estimates arrive.
- The low estimate of the severe loss comes from a vendor model, built on the few public loss cases: one hundred million dollars.
- The high estimate comes from a scenario panel of experts: six hundred million.
- The low add-on is one hundred divided by twenty five thousand, zero point four per cent of risk weighted assets.
- The high add-on is six hundred divided by twenty five thousand, two point four per cent.
- The range, high over low, is six hundred divided by one hundred, six times.
- With scarce loss data, nobody can say which is right.
- And even the larger add-on would not make Merrow's payments run again during an outage.

24 Reporting, sharing and testing

- Reporting: authority warned fast, sees common problems
- Sharing: one bank's warning protects the rest
- Obstacle: fear of reputation damage and liability
- Threat-led tests: real attack methods, real systems
- Obstacle: testing on real systems can disrupt

IN THE LESSON

- Next, reporting, sharing and testing.
- Mandatory incident reporting tells the authority quickly when a firm is hit, so it can warn others and see whether several firms share a problem.
- Information sharing passes details of attacks between firms, so that one bank's warning protects the rest.
- The obstacle is incentives.
- A firm fears that admitting an incident will hurt its reputation and invite lawsuits, so it shares late, or shares little.
- Threat-led penetration testing uses the methods real attackers are using, against the firm's actual production systems, because test copies can miss real weaknesses.
- But testing on systems that serve customers can itself cause the disruption it is meant to prevent, so it needs careful control.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

25 Example 7: a concentration limit

Limit: no provider may carry more than 40% of the market's payments

Share on Velnet now	30 + 25 + 15	**70%**
Limit for one provider	set by the authority	**40%**
Share that must move	70 − 40	**30 points**
Merrow leaves Velnet	70 − 30	**40%: meets limit**
Merrow joins Orrin	Cadell's 20 + 30	**50%: breach**

IN THE LESSON

- Now direct oversight of providers.
- Suppose the authority sets a concentration limit: no single provider may carry more than forty per cent of the market's payments.
- The share on Velnet now is thirty plus twenty five plus fifteen, seventy per cent.
- The limit for one provider, set by the authority, is forty per cent.
- So the share that must move is seventy minus forty, thirty percentage points.
- If Merrow leaves Velnet alone, Velnet falls to seventy minus thirty, forty per cent, which meets the limit.
- But where does Merrow go?
- If it joins Orrin, the obvious alternative, Cadell's twenty plus Merrow's thirty gives Orrin fifty per cent, a new breach.
- With only a few large providers, a limit can just move the concentration around.
- And Velnet itself may sit outside the regulator's reach, in another country.

26 Playbooks, resolution and exit plans

- Crisis playbook: who decides, who communicates
- Keeps payments moving; nobody improvises
- Recovery and resolution: critical functions continue
- Exit plans: how to leave a provider, and how fast
- Obstacles: rehearsal, many authorities, few substitutes

IN THE LESSON

- Three more tools prepare for the day something fails.
- A coordinated crisis playbook sets out in advance who decides, who communicates and how payments are kept moving in a system wide incident, so that authorities, banks and providers do not improvise.
- Recovery and resolution planning asks how each firm's critical functions would keep running if the firm itself failed or was badly damaged, including after a severe incident.
- Exit plans set out how a bank would move off a provider, and how long it would take.
- The obstacles are practical.
- Plans must be rehearsed to work, playbooks must span many authorities and countries, and an exit plan helps only if a substitute exists and the move is fast enough.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

27 Example 8: why insurance runs short

An insurer covers 10 banks, $100m each, and has $500m to pay claims

Policy limit per bank	10 banks insured	**$100m each**
Bad year, independent losses	2 banks × 100	**$200m**
Common outage hits all	10 × 100	**$1,000m**
Insurer's capacity	capital to pay claims	**$500m**
Shortfall in the common event	1,000 − 500	**$500m**

Moral hazard: full cover weakens firms' own defences

IN THE LESSON

- Last, risk transfer.
- An insurer covers ten banks, and holds five hundred million dollars to pay claims.
- The policy limit per bank, for each of the ten banks insured, is one hundred million dollars.
- If incidents are independent, a bad year might hit two banks: two times one hundred, two hundred million of claims.
- But a common provider outage hits all ten at once: ten times one hundred, one thousand million.
- The insurer's capacity, its capital to pay claims, is five hundred million.
- The shortfall is one thousand minus five hundred, five hundred million dollars.
- Correlated losses are exactly what limits insurance capacity.
- A public backstop could fill the gap, but full cover invites moral hazard: firms protected from loss spend less on their own defences.

28 Exam point: pair every tool with its limit

- Stress tests, capital: scarce data; no service restored
- Reporting, sharing: reputation and liability fears
- Provider oversight: perimeter and borders
- Insurance, backstops: correlation, moral hazard
- Live-system tests can disrupt; combine the tools

IN THE LESSON

- So here is the exam point for policy.
- Pair every tool with its limit.
- Stress tests and capital add-ons rest on scarce loss data, and capital absorbs losses but does not restore a stopped service.
- Reporting and sharing stall when firms fear reputation damage and liability.
- Oversight of providers meets a perimeter they sit outside, and borders they cross.
- Insurance and backstops are limited by correlated losses and moral hazard.
- And threat-led testing on real systems can cause the disruption it is meant to find.
- No one tool is enough, so authorities combine them, aiming at the common exposures that make an incident systemic.

29 Mistakes to avoid

- Equating ICT risk with cyber attacks
- Stopping at the direct cost of an incident
- Judging systemic risk by one firm's loss
- Assuming capital restarts a stopped service
- Naming a tool without its obstacle

IN THE LESSON

- Before the quiz, here are the mistakes to avoid across the whole topic.
- Do not equate I C T risk with cyber attacks: accidents, faulty changes, legacy systems and provider failures count too, and they were most of Merrow's loss.
- Do not stop at the direct cost of an incident, because liquidity, funding and confidence effects can be far larger.
- Do not judge systemic risk by the size of one firm's loss; look for common exposure, connectedness and confidence.
- Do not assume capital solves cyber risk, because it cannot restart a stopped service.
- And do not name a tool without its obstacle.

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

30 Try three quick questions

1. Engineer's faulty change halts card payments for 4 hours. Cyber? Property?
   Answer: ICT but not cyber: no intent. Availability.
2. Must pay $2.5bn; cash $2.0bn; $0.8bn incoming is trapped. Shortfall?
   Answer: 2.5 − 2.0 = $0.5bn
3. Provider concentration met by a capital add-on alone. What is missed?
   Answer: Capital does not restore service: add exit plans, substitutes, oversight.

IN THE LESSON

- Try three quick questions, then listen to the answers.
- Question one.
- A bank's own engineer makes a faulty change that halts card payments for four hours.
- Is it cyber, and which property is hit?
- It is I C T risk but not cyber, because nobody meant harm, and it hits availability.
- Question two.
- A bank must pay two point five billion dollars today, holds two billion of cash, and expects zero point eight billion of incoming payments, which an outage traps.
- What is the shortfall?
- Two point five minus two, zero point five billion dollars.
- Question three.
- An authority answers a provider concentration with a capital add-on alone.
- What does that miss?
- Capital absorbs losses but does not restore the service.
- It needs exit plans, substitutes and oversight of the provider.

Summary notes for the Charta whiteboard lesson. Figures are from the lesson's made-up examples.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.