## Cybersecurity in Finance: The Connectivity Paradox

We built systems to protect our money digitally – but every new digital connection is a new door for attackers

Digital Finance

# Why Does Making Banking More Convenient Also Make It More Dangerous?

**The Connectivity Paradox**

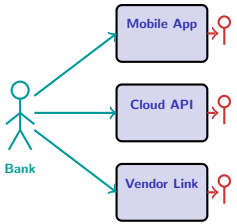
Financial institutions are racing to digitize everything – mobile banking, cloud computing, open APIs, real-time payments. Every new digital channel makes services faster, cheaper, and more convenient for customers.

**What digitization delivers:**

- Instant payments across borders at near-zero cost
- Open banking APIs that let third-party apps access your account
- Cloud infrastructure that scales on demand
- Mobile-first services available around the clock

**What digitization also creates:**

- Every API endpoint is a potential entry point for attackers
- Every cloud vendor is a dependency you cannot fully control
- Every mobile device is a node on a network you do not own
- Every real-time connection means real-time exposure




*Every door you open for customers, you open for attackers.*

**Financial digitization is a double-edged sword – the same connectivity that enables instant payments creates the attack surface that criminals exploit.**

# How Many of Your Financial Accounts Could Be Reached Through a Single Stolen Password?

## Quick Exercise

Open your phone. Count how many financial apps you have – banking, payments, investment, insurance, crypto. Now ask yourself:

**1.** How many of these apps use the same email address for login?

**2.** If someone gained access to your email account right now, how many of those financial services could they reset the password for?

**3.** When was the last time one of your service providers emailed you about a "security incident" or "data breach"?

Most people have between five and fifteen financial accounts connected to a single email address. A breach at any one service – even a non-financial one – can give attackers the foothold they need to reach the others.

This is the **connectivity paradox at the personal level**: the convenience of a single digital identity (one email, one phone, one password manager) is also the single point of failure. Financial institutions face exactly the same paradox at an institutional scale – with thousands of connected systems instead of fifteen apps.

**Bring your count to class.** We will use it as a running example throughout the lecture.

---

**Most people reuse passwords across services – which means a single breach anywhere can cascade into a financial breach everywhere.**

# What Types of Cyber Threats Actually Hit Financial Institutions?

| Dimension | Opportunistic Crime | Organized Cybercrime | State-Sponsored Attack |
|---|---|---|---|
| Target | Any vulnerable system | Financial institutions | Critical infrastructure |
| Goal | Quick profit | Large-scale theft | Disruption, espionage |
| Method | Phishing, malware | Ransomware, SWIFT fraud | Zero-day exploits, supply chain |
| Sophistication | Low | Medium–high | Very high |
| Typical damage | Thousands | Millions | Systemic disruption |
| Detection | Days | Weeks–months | Months–years |
| Recovery | Replace credentials | Rebuild systems | National coordination |

**Pattern to notice:** Read from left to right. As sophistication rises, detection time lengthens and damage scales from individual to systemic. The most dangerous attacks are the ones you do not know about yet.

**Why finance is a prime target**

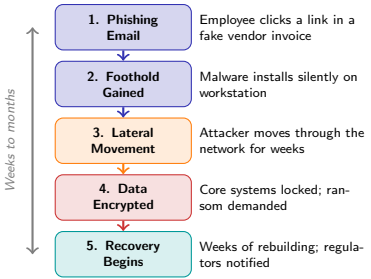
- **Money is digital** – attackers can steal directly, not physically
- **Data is valuable** – customer records, trading strategies, compliance data
- **Uptime is critical** – even minutes of downtime cost millions in lost trades
- **Trust is fragile** – a single publicized breach can trigger customer flight

**The insider dimension**

- Not all threats come from outside – employees with legitimate access can cause the most damage
- Insider threats are harder to detect because the attacker already has the keys

**The threat landscape in finance is not a single risk – it is a spectrum from opportunistic crime to state-sponsored warfare, each requiring different defenses.**

# Follow One Ransomware Attack from First Click to Last Recovery Step




**Anatomy of a financial cyber attack**

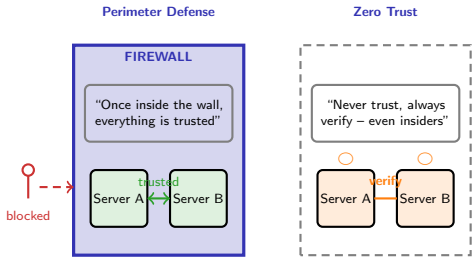
- **Entry** is almost always human – a clicked link, a reused password, a misconfigured server
- **Dwell time** is the silent phase: the attacker is inside but has not struck yet, studying the network
- **The decision point** comes when the attacker decides to encrypt, exfiltrate, or both
- **Recovery** is not just technical – it includes regulatory reporting, customer notification, and reputation repair

**What makes financial attacks different:**

- Attackers study payment systems before striking
- They time attacks to maximize disruption (month-end, market close)
- They threaten to release customer data to force payment

**The average time from initial compromise to detection in financial services is measured in weeks, not hours – attackers often have free rein long before anyone notices.**

# Should a Bank Defend at the Perimeter, Inside the Network, or Both?




**Two philosophies of defense**

- **Perimeter defense** builds a wall and trusts everything inside – fast but brittle. One breach and the attacker roams freely.
- **Zero trust** assumes the attacker is already inside. Every request, every user, every device must prove its identity – slower but resilient.

**Why finance is shifting to zero trust:**

- Cloud computing dissolves the perimeter – there is no "inside" anymore
- Remote work means employees connect from everywhere
- Open banking APIs invite third parties into the network by design
- Regulators increasingly expect continuous verification, not one-time checks

**The honest answer:** most banks run both models simultaneously – legacy systems behind firewalls, new systems on zero trust.

**The shift from perimeter defense to zero trust reflects a deeper lesson: if you cannot prevent every breach, you must assume the attacker is already inside.**

# What Happens When Your Cloud Provider Goes Down and Takes Half the Banking System With It?

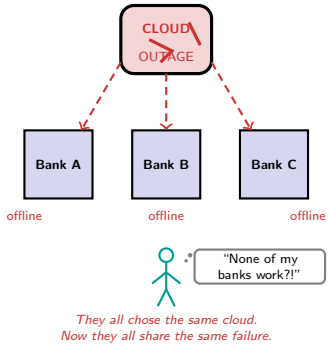
**The concentration risk nobody planned for**
Financial institutions moved to the cloud for good reasons – scalability, cost efficiency, faster deployment. But a handful of cloud providers now underpin the majority of the financial system.

**The failure cascade:**

- A cloud provider suffers an outage – not a cyberattack, just a configuration error
- Payment systems at dozens of banks go offline simultaneously
- Customers cannot access accounts, merchants cannot process transactions
- Regulators discover they have no authority over the cloud provider
- The bank's recovery plan assumed the *bank* would fail, not its *vendor*

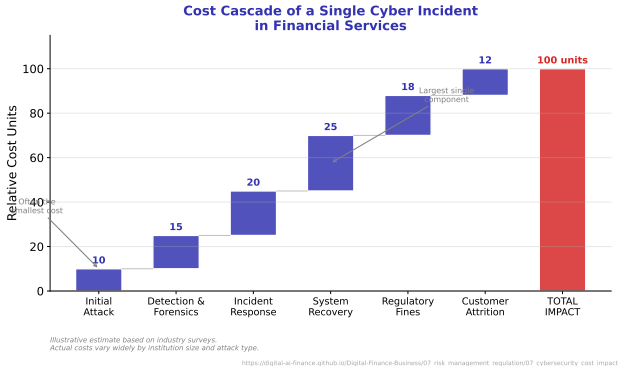
**Third-party risk is cyber risk:**

- Vendors have access to sensitive data and critical systems
- A breach at a vendor becomes a breach at every client
- Supply chain attacks target the weakest link – often a small subcontractor
- The EU's DORA regulation now requires banks to monitor third-party ICT risk




**Concentration risk in cloud computing is the new systemic risk – when everyone depends on the same provider, a single failure becomes everyone's failure.**

# How Does the Cost of a Single Cyber Incident Cascade Through a Financial Institution?



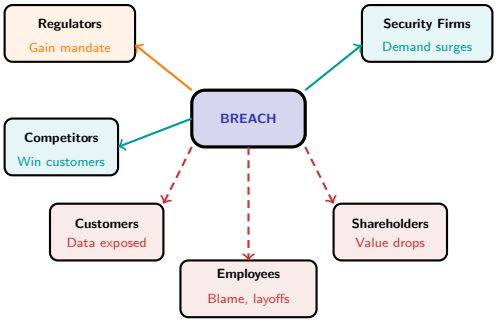

**Reading the waterfall**

- The **initial attack** is often the smallest cost – ransomware payments or immediate damage
- **Detection** takes weeks, and every day of dwell time adds forensic cost
- **Response** includes customer notification, legal counsel, and crisis management
- **Recovery** means rebuilding systems, restoring data, and resuming operations
- **Regulatory fines** compound the damage – especially under data protection laws
- The **total** is typically several times the initial attack cost

**The hidden cost:** reputational damage and customer attrition are not in this chart – they can exceed all visible costs combined.

**Illustrative estimate based on industry surveys. The direct cost of an attack is often dwarfed by the downstream costs of detection, response, recovery, and regulatory penalties.**

# Who Wins and Who Loses When a Major Financial Institution Is Breached?




**The same event, different experiences**

**Harmed:**

- **Customers** lose data, face identity theft risk, and bear emotional cost
- **Shareholders** see stock price drop and face litigation
- **Employees** face blame, investigation, and potential layoffs in restructuring

**Benefit:**

- **Security firms** see immediate surge in demand for their services
- **Competitors** gain customers fleeing the breached institution

**Complex:**

- **Regulators** gain political mandate for stricter rules – but also face questions about why they did not prevent it

**The same breach creates winners and losers – and the people who bear the most harm (customers, small institutions) have the least power to prevent it.**

# Four Questions That Reveal Any Financial Institution's True Cyber Resilience

When you read about a financial institution's cybersecurity posture – or when you evaluate one as an investor, regulator, or employee – ask these four questions:

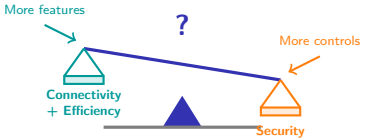
**1. How fast can they detect a breach?**
Not "do they have monitoring" but what is the actual mean time to detection? Days is bad. Hours is baseline. Minutes is good.

**2. Who is responsible when it goes wrong?**
Is there a named person with board-level authority for cyber risk? Or is it buried three levels down in IT?

**3. What happens when their biggest vendor fails?**
Do they have tested fallback plans for cloud outages, or does one vendor failure take them down?

**4. When did they last test recovery – and did it work?**
Recovery plans that exist only on paper are not plans. Have they run a realistic drill in the past year?

**The framework:** These four questions map to the DORA regulation's core pillars – detection, governance, third-party risk, and resilience testing.




**Every institution claims to take cybersecurity seriously. These four questions separate the ones that mean it from the ones that do not.**

# Your Challenge: Evaluate a Financial Institution's Cyber Resilience

## Your Challenge

**The scenario:** A mid-sized bank announces it is migrating all core systems to a single cloud provider. It promises faster services, lower costs, and "state-of-the-art security." The CEO says: "Our customers' data has never been safer."

**Apply the four questions from the previous slide:**

| Question | Your Assessment |
|---|---|
| 1. How fast can they detect a breach? | ..... |
| 2. Who is responsible when it goes wrong? | ..... |
| 3. What happens when their cloud vendor fails? | ..... |
| 4. When did they last test recovery? | ..... |

**Discuss with your neighbor:**

- What is the biggest risk you identified in this scenario?
- What would you need to know before trusting the CEO's statement?
- Where do you disagree? That disagreement reveals the tension between convenience and security.

**The four-question framework works for any institution – bank, insurer, payment provider, or crypto exchange. Practice it once, and you can apply it anywhere.**