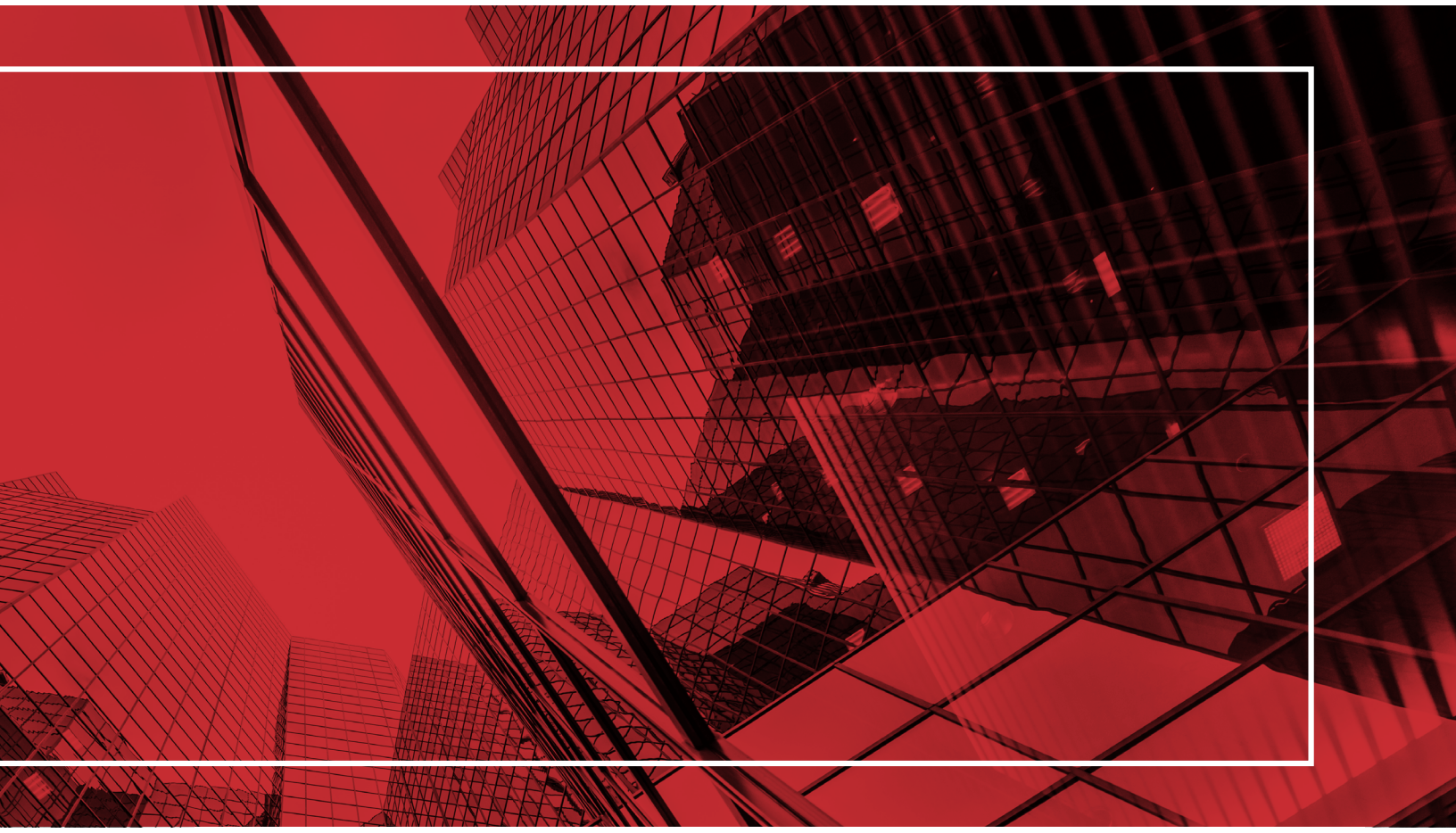
CYBER RESILIENCY: LEADING THE WAY THROUGH ADVANCED PREPARATION



CAPCO

THE FUTURE. NOW.

With an increase in connected devices, an ever-growing number of online services, and the vast amounts of data that individuals and corporations store on internet-connected systems, cybersecurity is as relevant today as ever.

Events such as the Equifax data breach (2017, affected over 146 million Americans), Yahoo! account breach (2013, three billion Yahoo! Accounts impacted across multiple services), and the Sony Pictures data hack (2014, 100 terabytes of data and 47,000 Social Security Numbers) have made headlines in recent years.[1]

Cyber-attacks and worms can widely spread within hours of appearing and bring down the computer infrastructure of entire firms in under a minute. In 2017, the 'NotPetya' cyber-attack brought down the network of State Savings Bank of Ukraine, Ukraine's largest bank, within 45 seconds and crippled multinational firms including Maersk, Merck, FedEx and Mondeléz International causing an estimated total of $10 billion in damages.[2]

Although these incidents have been troubling for both the companies and individuals who had data compromised, they resulted in increased cyber awareness. Companies are taking more proactive measures to secure their infrastructure and make their detection and resolution processes more robust. Cybersecurity is critical to financial institutions. Cyber-attacks are no longer a matter of 'what if,' but are now a reality to be dealt with as a part of daily operations.

As part of the Payments Practice at Capco, we have been working with Canadian financial institutions to create cyber resiliency processes, to follow are some of our insights and learnings from our work.

1. GOVERNANCE THROUGH FORMALIZED PROCESSES, ROLES AND RESPONSIBILITIES

The detection, investigation and response to cyber incidents must go through formal processes that include proper documentation and open communication with all team members. After a cyber event is detected, time is of the essence, and prompt action is required to investigate the cause of the event, its implications, and create a remediation plan.

As cyber events often impact more than one team, having the appropriate governance and structure in place is essential, so that cross-functional and task-force teams can be formed to remediate the event successfully.

[1] https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks

[2] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

2. CHANNELS FOR INFORMATION FLOW

As a follow up to point number one, when a cyber incident is suspected, it's essential to share information with the right teams and individuals – both within the organization and outside. You need to develop distribution lists for sharing within the organization so that you notify the right individuals if you suspect a cyber incident. When an event occurs, even if not confirmed as cyber, it is good practice to inform other teams, essentially saying 'we notice something unusual and we're investigating. Let us know if anything is flagged on your radar too.' That way, other teams can help diagnose the event, and if confirmed as cyber, will be able to respond to it sooner.

In some cases, a cyber-attack can affect more than one financial institution – either directly or indirectly. For example, one large bank being unable to send and receive payments for a prolonged period can cause a systemic loss of liquidity. Our findings show that in such situations, it is vital to notify other FIs that they may be affected as soon as you identify the risk, for them to react and remediate appropriately. Similar to the communication within the affected FI, cross-FI and FMI communication will need to occur through pre-defined channels and distribution lists.

3. REHEARSAL OF APPROPRIATE HANDLING OF EMERGENCY SITUATIONS

Rehearsing the appropriate procedures, in place, when a cyber incident occurs can significantly improve the outcome of actual cyber situations and can also help solidify existing processes. Simulations and ethical hacks are two ways you can rehearse potential cyber situations.

In a simulation, you assemble a cross-functional team to run through a scenario and its corresponding actions. Simulations can be practical (live) or table-top (theoretical exercises that test the understanding of actions to take, but do not involve working with systems or other external personnel).

In comparison, ethical hacks are practical exercises in which you simulate a cyber-attack such as phishing in a production environment, and responders are usually not aware that it is a test. Ethical hacks test how easy it is to penetrate the company's security mechanisms and employees' susceptibility to cyber.

We found that both simulations and ethical hacks helped participating FIs detect gaps in their processes and as a result led to learnings and actions to enhance their processes and make them robust.

4. NECESSITY FOR A CONTINGENCY PLAN – AND A CONTINGENCY TO THE CONTINGENCY

Setting up a robust business continuity plan (BCP) is essential for the organization to be able to function in the event of a failure of its primary site or systems.

Although the vast majority of organizations we work with have a BCP in place, we discovered that some have struggled with the question "How long can your organization survive when running in BCP?" We found that BCP plans work well for specific scenarios, such as regional outages, and for a pre-defined timeline, but what happens when incidents are systemic with a longer timeline, or when the situation doesn't fit into one of the known situations?

For those cases, setting up an alternate BCP option, which you activate in the event that the bank is unable to function on the primary BCP, can allow it to survive for more extended periods of time while normal operations are restored. What this alternate BCP looks like can vary from bank to bank – it depends on the FIs in-house resource capacity, technological capabilities, funds available for investment, and risk tolerance. The alternate BCP needs to be scalable for longer periods of time, reliable for operational stability, and secure (air-gapped) to avoid the risk of contamination of systems, applications, infrastructure and data. In many cases, organizations may choose an alternate BCP option that is a combination of in-house and outsourced capabilities.

BRINGING IT ALL TOGETHER

Financial institutions can increase their resiliency to cyber-attacks through in-depth planning, creating networks for information flow within the organization and with other industry participants, regularly rehearsing emergency situations, and setting up multi-level contingency plans.

Although cyber-attacks cannot be predicted, through proper preparation, the bank's response to them can be managed well and recovery time can be improved.

For more information, please contact us at canadapaymentspractice@capco.com

AUTHOR

Reuben Piryatinsky,
Principal Consultant, Capco Toronto

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, finance, risk & compliance and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on **Twitter**, **Facebook**, **YouTube**, **LinkedIn**, and **Instagram**.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
THE FUTURE. NOW.