CYBER-ATTACK: PREPARING FOR THE INEVITABLE

For the financial services industry, it's not a matter of if, but when, a large-scale cyber-attack will occur. In fact, nearly one of every four (24%) cyber breaches in 2017 affected a financial services organization, according to the Verizon 2017 Data Breach Investigations Report, making the sector the number one target for cyber-attacks. Perhaps even more troubling is that the rate of successful cyber breaches per firm in the financial services sector alone jumped to 125 in 2017, up from 40 in 2012 - that's a 200% increase in just five years.

And those breaches are getting more costly. According to Accenture's 2017 Cost of Cyber Crime Study, the average total cost of a cyber-attack per firm reached nearly $18.3 million, an increase of $7.32 million since 2014.

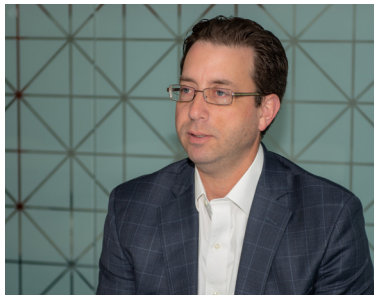
The complexity of the financial services industry, the interconnectedness of individual players, and the introduction of new and innovative technologies further heighten the risk of a large-scale cyber-attack on the financial sector.

In March, DTCC and Oliver Wyman released a white paper highlighting key initiatives that are essential to mitigating the systemic consequences of a large-scale attack.

Recently, Stephen Scharf, DTCC Chief Security Officer, and David LaFalce, DTCC Executive Director and Global Head Business Continuity & Crisis Management, discussed how the industry can advance those proposals outlined from the paper, taking concepts and making them reality.

Q.: WHAT CONSIDERATIONS MUST BE MADE TO MITIGATE THE SYSTEMIC CONSEQUENCES OF A LARGE-SCALE CYBER-ATTACK?

David: Most important is a well-coordinated cross-industry effort that allows for a collective response and recovery plan. The industry currently lacks standards around key considerations. Individual entities know that they must follow recovery protocols for their most critical services before they can resume operations after an impact. But in a sector outage that



Stephen Scharf
DTCC Chief Security Officer

> "A prime example of industry coordination is contingent service arrangements or interoperability."

DTCC
Securing Today. Shaping Tomorrow.®

spans across firms, there may be a different order of operations to follow; firms need to be flexible. In addition, there needs to be a definition of when an entity is considered safe to rejoin the ecosystem. This is something being worked on through a SIFMA effort.

Q.: HOW WOULD A CROSS-INDUSTRY APPROACH HELP TO MITIGATE THE IMPACT OF A LARGE-SCALE CYBER-ATTACK?

Stephen: A cross-industry approach would identify collective actions to be taken upon the detection of a large-scale cyber-attack, based on a set of standardized criteria that is tailored to specific cyber-attack scenarios.

There are four key benefits to this approach. *First,* it improves resilience of the overall financial system by ensuring firms are held up to a minimum set of acceptable standards and minimizing the threat of contagion. *Second,* it creates clearly defined and readily available protocols that increase speed of reaction to cyber-attacks. *Third,* it increases customer / investor confidence, driven by the knowledge that the industry is following a set of commonly agreed upon set of standards. *Lastly,* it increases transparency and confidence between institutions.

Q.: INDUSTRY COORDINATION IS CRITICAL TO RESPONDING TO AND RECOVERING FROM A CYBER-ATTACK. CAN YOU GIVE US AN EXAMPLE OF THAT INDUSTRY COORDINATION?

Stephen: First, let me say I agree with your opening statement about the importance of industry coordination. A prime example of industry coordination is contingent service arrangements or interoperability. Given the complexity and broad scope of potential impacts of large-scale cyber-attacks, such as the outage of key players or compromise of backups, no single entity has all the required capabilities and capacities to address all possible attack vectors and vulnerabilities. Regardless of the level of preparedness, there may be situations where a key payment, clearing, and settlement provider is unable to fulfill its services for an extended period of time.

Q.: THE DTCC-OW CYBER WHITE PAPER CALLS FOR FURTHER CONSIDERATION OF CONTINGENT SERVICE ARRANGEMENTS. HOW DO YOU ENVISION SUCH ARRANGEMENTS WORKING?

David: There isn't a one-size fits-all approach for contingent service arrangements. To that end, we see three potential operating models for the development of arrangements. The first model is interoperability. We see this in the exchanges where if one exchange is down, the others are able to provide the platform for the majority of the symbols. In the second version, there would be arrangements between existing institutions to provide mutual assistance in support of critical activities during the time of need. Lastly, we could create an industry utility designed to perform services to several financial institutions. An example of this is the Sheltered Harbor effort.

Regardless of the model, these arrangements offer a number of key benefits. They would increase the resilience of the financial services sector and reduce instability and economic gridlock during a large-scale

David LaFalce
DTCC Executive Director and Global Head Business Continuity & Crisis Management

> "The industry currently lacks standards around key considerations. Individual entities know that they must follow recovery protocols for their most critical services before they can resume operations after an impact."

DTCC
Securing Today. Shaping Tomorrow.®

cyber-attack. They'd also reduce the potential for contagion by reducing the likelihood of a critical player rejoining the financial system prematurely, due to the absence of a substitute service provider. We can't discount that another great benefit of the contingent service arrangements is that it will increase customer and investor confidence, driven by the knowledge that the industry has implemented multiple layers of protection to facilitate continuity of critical industry activities.

Q.: WHAT ARE THE NEXT STEPS?

Stephen: I hope our white paper will act as a rallying cry. Now it's time for the industry to work together to turn these concepts into realities. Some efforts are already underway but for those that are not, the industry must assign ownership and responsibilities for the initiatives. The appropriate industry stakeholders must mobilize and detail each initiative, including scope, ownership structure, execution model, and enforcement mechanism. They need to develop a structured implementation plan, and implement initiatives.

That said, the industry cannot go it alone. The public sector needs to step in when legislative support is necessary to implement industry-wide and cross-border efforts, both in terms of providing incentives and helping resolve roadblocks related to misaligned legislative frameworks.

We have meetings scheduled with different individual groups (e.g., FSARC, SIFMA) and we are leveraging the DTCC membership to establish common understanding on what needs to be prioritized. We are also working to further refine our internal practices around preparing for and combatting cyber-attacks.