

# ACCELERATING A LARGE CYBERSECURITY PROGRAM

Trexin helped a super-regional financial services company advance delivery of a \$20M cybersecurity program.

## BUSINESS DRIVER

Our Client, a financial services company with nearly \$70B in total assets, experienced a string of Distributed Denial of Service (DDoS) attacks and evolving Advanced Persistent Threat (APT) activity, prompting the creation of a Cybersecurity Program aimed at fortifying the mitigation, defense, and response mechanisms used to protect the company and its customers. Amid heightened collaboration with US Government entities, including the FBI, the Chief Information Security Officer (CISO) had concerns about the delivery speed of the Program and asked Trexin to provide senior technical delivery resources seasoned in navigating complex and process-heavy environments to re-baseline the Program and meet Board expectations by accelerating delivery of Program objectives.

## APPROACH

Trexin applied a Defense in Depth cybersecurity approach to address all major levels of the internal and external network infrastructure. The Program objectives were organized into logical workstreams to allow an “early-and-often” deliverable schedule with the end-state solution being achieved when all components were delivered. This allowed for a relatively independent schedule for each deliverable that minimized dependencies and unnecessary slowdowns. Cloud-based services from multiple vendors were contracted to analyze and process external traffic with a goal of 99% effectiveness prior to inbound entry to the customer network. The anticipated level of residual DDoS traffic downstream of the cloud was the new target focus of the effort. Bandwidth capabilities were increased throughout the infrastructure to provide greater per-second processing of network traffic to increase the probability of the customer transaction completing as intended during times of an attack. A Big Data solution based on Hadoop and Cisco UCS hardware was created to store all network data for analysis and correlation of seemingly benign activities that traditionally do not trigger alerts by themselves. Advanced malware appliance and software solutions were deployed at all layers of the environment to monitor and protect against both inbound attacks as well as outbound command/control communication and exfiltration of data.

## RESULTS

Driven by Trexin’s leadership, the Cybersecurity Program began completing deliverables on nearly a monthly basis for the duration of the Program, incrementally protecting the company in route to the full end-state solution. Several organizational units were realigned to more effectively manage the vast array of components comprising the solution. And the preexisting Cybersecurity strategy was exponentially strengthened to provide a stable, long-term foundation for keeping current with the constantly evolving threat landscape which is now being continually improved to address seemingly daily advances by Cyber criminals.

### Fending Off Cyber Criminals with a “Defense in Depth” Program



Our Client was experiencing a string of cyber attacks and/or threats. They required a program set in place to protect both their customers and the company at large.

### Defense in Depth

Trexin applied a cybersecurity approach that addressed all major levels of internal and external network infrastructure.

- Independent schedule for each deliverable
- Vendors to analyze and process external traffic
- Bandwidth capabilities increased
- Big Data solution for forensic analytics
- Advanced malware appliance and software solutions deployed



### Diminishing the Threat from Cyber Criminals

Trexin’s leadership helped to deliver results and advances in the Client’s Cybersecurity Program:



Deliverables completed nearly monthly for duration of Program



Current Cybersecurity strategy strengthened and continues to be improved upon



Several organizational units were realigned; effectively managing the solution’s components

## CONTACT US

Financial Services Practice  
fs@trexin.com  
www.trexin.com