Wembley
Partners

CASE STUDY

E-COMMERCE COMPANY AVOIDS MASSIVE LOSSES

E-commerce businesses can be especially vulnerable due to mission-critical high availability requirements and supply chain complexities. We were asked to help with operationalizing a Cyber Incident Response program, which turned out to be a timely decision.

Engagement Context

Evolving with the times

A North American E-commerce and manufacturing company, specializing in distributing consumer electronics was concerned regarding their ability to adequately respond to a cyber incident. While perimeter controls and basic attack detection capabilities were in place, both technical and executive teams had little knowledge when it came to handling specific cyber attack scenarios. Communication between business functions was lacking as well, as cyber was historically perceived as an IT problem.

Wembley Partners was engaged to assess the current state of the business' preparedness to respond to a cyber incident, identify improvement opportunities, operationalize a detailed cyber incident response program (complete with highly detailed Plan and Playbooks), and perform simulation training sessions with the technical (IT) and executive teams.

Services
Cyber Incident Response Planning

Key Success Metric
Ability to internally detect and respond to a cyber incident within 2 hours

Value Delivered
Over $4,200,000

Our Work

Many organizations recognize that developing a Cyber Incident Response Program using only the internal resources is a costly task. By joining efforts with external subject matter experts at Wembley Partners, the client was able to operationalize the program from the ground up in under 3 months.

Impressively, the entire engagement was carried out remotely in accordance with social distancing requirements, and provided a total of over $320,000 in savings when compared to an estimate of using only internal expertise.

1

Current State Assessment

Wembley Partners' consultants conducted a detailed analysis of the current infrastructure, performed a Cyber Threat Intelligence research, held 20+ stakeholder interviews, and compiled a detailed report outlining risk-scored Crown Jewels, attack vectors, and more.

2

Cyber Incident Response Plan (84 pages)

Based on the Current State Assessment and existing Wembley accelerators, we've been able to create a detailed, fully custom IR Plan in under 3 weeks covering the entire program, RACI, 3rd party collaboration and containing report and communication templates.

3

8 Cyber Incident Response Playbooks

Step-by-step Playbooks (Ransomware, DDoS, 3rd Party Compromise and more) were created to further detail the IR Plan and contained practical actions across Identification, Containment, Eradication, Recovery, and Lessons Learned stages of the SANS incident lifecycle.

4

Cyber Crisis Simulation ("Tabletop")

Practice makes perfect. We've conducted two interactive full-day cyber crisis simulation sessions ("Tabletop Exercises") with technical and executive teams that covered customized scenarios tailored specifically to our client and their E-commerce business.

Outcomes

1

Wembley Partners created 19 artifacts, such as the Crown Jewel list, risk-scored Asset Inventory, Communications Matrix, etc. that have not only been crucial to the success of the Cyber Incident Response program, but assisted with overall business risk planning.

2

Over 200 pages of Incident Response Plan and Playbooks were created and undergone multiple review sessions with key stakeholders. All relevant team members received supporting materials (e.g. cheat sheets) and a detailed walkthrough training with Q&A.

3

Wembley Partners delivered over 30 incident response accelerators (communications and report templates, digital forensics tools, legal guidance, breach notification templates, etc.) maximizing the efficiency of the Cyber Incident Response process.

4

All staff that would be involved in an incident of any significance received in-depth real-time simulation training via the Tabletop Exercise, twice. The interactive scenario was bespoke the client, based on the Cyber Threat and Current State assessments.

5

During the closing phase, a ransomware drive-by download incident has been reported via a newly established process. Following the steps outlined in the new Ransomware playbook, the client's IRT was able to contain the malware to 3 staff laptops, avoiding costly downtime.

6

In addition, a 2-year Cybersecurity Maturity Roadmap was created, containing quarterly milestones and 5 distinctive work streams, with the goal of optimizing budget spending and prioritizing gaps discovered during the Current State Assessment.

By The Numbers

8

23

$4.2M

Assets

8 detailed playbooks created, covering prioritized attack scenarios aligned to crown jewels

Skills

23 Incident Response and Executive Crisis Management team members trained

Bottom Line

$4.2M in sales downtime losses prevented due to operationalized IR program

Additional Metrics

Client feedback

We went to Wembley to get us ready for an incident <...> all of the deliverables were of extremely high quality, and the learning curve during the Tabletop was fantastic. The CEO is now convinced this is the best idea since sliced bread. We will likely do these at least annually going forward.

	Time to resolve an incident (hrs)	IR Team Readiness (1-10)
Before WP	32	4
After WP	8	9

IT Team Members Trained	Success Achieved (9 participants)
14/14	100%

Self-assessment metrics

About Us

50+
Clients

$180M+
Value Created

1
Firm

We are a bespoke cybersecurity services and products firm with offices in Canada, UK and the US. Since our inception in 2017, we provide tailored Cyber Threat Intelligence-led services and products to businesses across the US, UK and Canada, specializing in high touch high-impact strategic initiatives, such as Cyber Incident Response Program operationalization, Cybersecurity Program Design and Implementation and Managed Detection & Response.

Our Brand

EXCELLENCE

Our clients repeatedly commend our professionalism, agility, outstanding branding and quality of deliverables.

EXPERTISE

Celebrated cyber risk and business experts on board, with 34 certifications and 200+ years of experience combined.

GROWTH

We've assembled an outstanding team of 17 professionals and acquired over 50 major clients, including Fortune 500.

We come to work every day to help our clients answer the toughest questions and resolve the most expensive problems when it comes to cyber risk. This is precisely why we are very particular about the calibre of our consultants. They are all senior industry professionals with 10-25 years in the field, specializing in one or more areas of cyber risk, and their combination of subject matter expertise and business acumen makes our firm stand out from typical quantity-over-quality models. Our Partners' combined expertise includes leading mission-critical projects exceeding $200M in budget and helping 50+ global clients across financial, healthcare, high-tech and government sectors in 8 countries.

Thank You.

Our expertise is your success.

Americas

Canada
340 King Street East, 4th Floor
Toronto, Ontario
info@wembleypartners.com
Tel: +1 (647) 952 0920

USA
Coming soon!
Dover, Delaware
info@wembleypartners.com
Tel: +1 (415) 949 2051

Europe, the Middle East & Africa

United Kingdom
Hub8, The Brewery Quarter
Cheltenham, Gloucestershire
info@wembleypartners.com
Tel: +44 07951 814580