Cyber Incident Response

Planning, Playbooks and Crisis Simulation Training

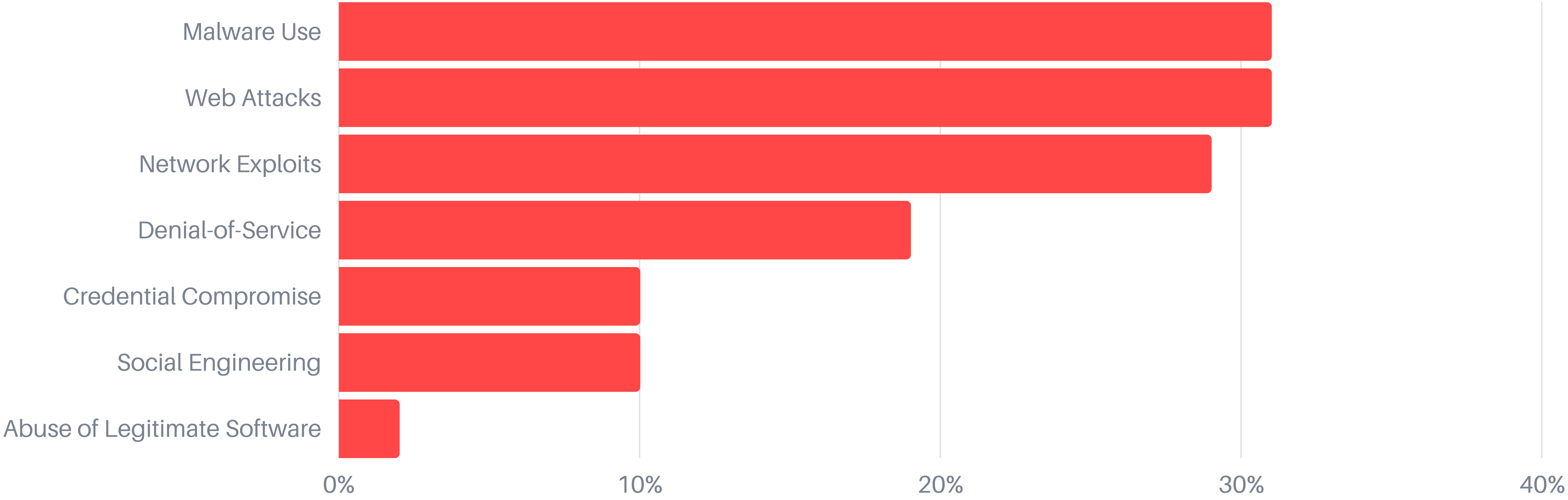
Once crisis strikes, does your team know exactly what to do?

#expensiveproblem

Why We Care

You might have heard the "*with cybersecurity, it isn't a matter of **If**, but **When***" cliché. Unfortunately, the phrase is popular for a simple reason: it's true.

Over 6,000 businesses across the globe suffered a cyber breach last year. Perhaps yours was one of them, or perhaps it will be this year. 7.9 billion records. Over $23,500,000,000 in losses. All it takes is any one of these:



Why We Act

We know that a cyber incident **will** happen, and you should too. With an average cost of a breach now near $3.86M, it pays to be prepared - and the key is an operationalized and efficient Cyber Incident Response program.

Ad-Hoc Cyber Incident Response (IR)

- Potential non-compliance with local or global breach and/or Privacy regulations, leading to regulatory fines and highly detailed audits
- Added levels of complexity and stress across all functions during an incident as communications, next steps and overall course of action are unclear
- Difficulties in triaging the incident and determining the level of urgency/impact due to the lack of defined frame of reference (eg. asset criticality, classes of data)
- Ineffective identification, containment and eradication efforts due to IT team's potential unfamiliarity with particular operating procedures as related to specific cyber attack scenarios

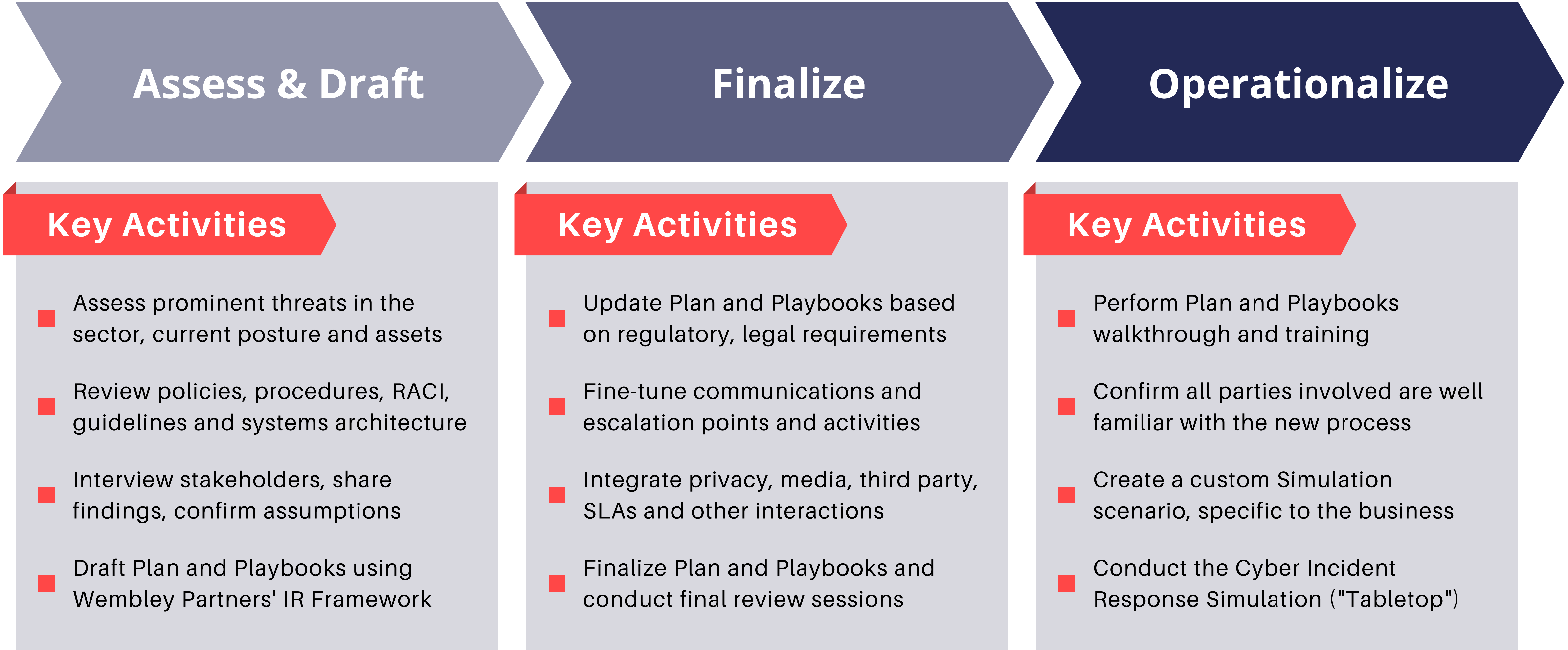
VS

Fully Operational IR Program

- Clearly outlined regulatory requirements, specific notifications guidance, compliance actions and communications templates
- Clearly defined escalation points, steps, interactions and collaboration across all functions and levels - from technical to executive crisis management
- Clear incident scoring matrix, allowing the team to rapidly determine and track incident severity continiously throughout the remediation process
- Teams across functions (communications, legal, IT, business etc.) are trained to perform optimal actions in case of a cyber incident, increasing the effectiveness of the containment efforts and the overall response

Our Approach

Building on our consultants' expert knowledge of cybersecurity and digital forensics, as well as business acumen and enterprise change management, we deploy a fully operationalized bespoke Cyber Incident Response program in your organization in 3 phases.



Assess & Draft

Key Activities

- Assess prominent threats in the sector, current posture and assets
- Review policies, procedures, RACI, guidelines and systems architecture
- Interview stakeholders, share findings, confirm assumptions
- Draft Plan and Playbooks using Wembley Partners' IR Framework

Finalize

Key Activities

- Update Plan and Playbooks based on regulatory, legal requirements
- Fine-tune communications and escalation points and activities
- Integrate privacy, media, third party, SLAs and other interactions
- Finalize Plan and Playbooks and conduct final review sessions

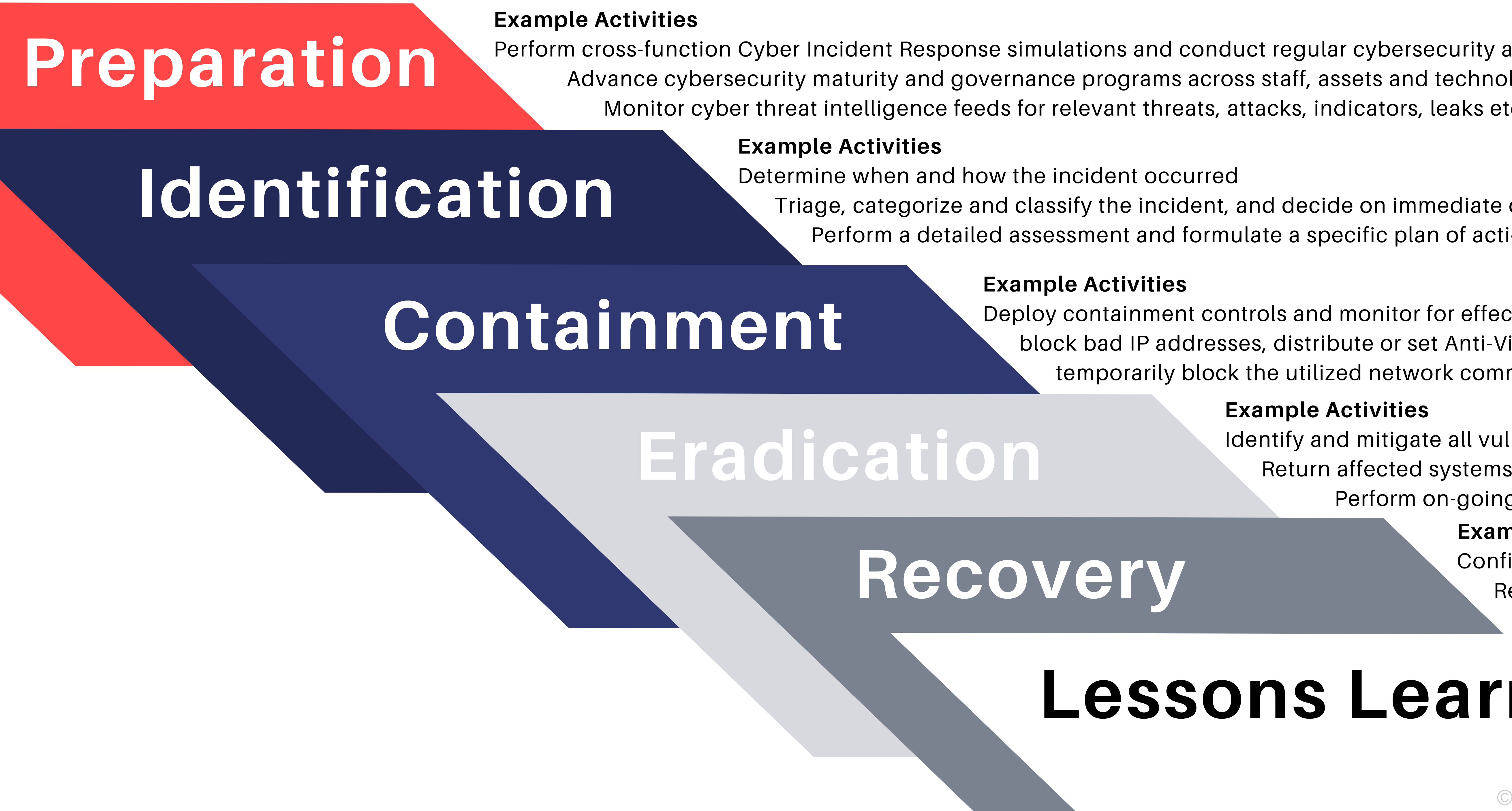
Operationalize

Key Activities

- Perform Plan and Playbooks walkthrough and training
- Confirm all parties involved are well familiar with the new process
- Create a custom Simulation scenario, specific to the business
- Conduct the Cyber Incident Response Simulation ("Tabletop")

Our Framework

Wembley Partners' Plan and Playbooks detail a customized industry-leading Cyber Incident Response process heavily based on the 6-stage SANS methodology with additional inputs from the NIST cybersecurity framework.



Preparation

Example Activities

Perform cross-function Cyber Incident Response simulations and conduct regular cybersecurity awareness training

Advance cybersecurity maturity and governance programs across staff, assets and technologies

Monitor cyber threat intelligence feeds for relevant threats, attacks, indicators, leaks etc.

Identification

Example Activities

Determine when and how the incident occurred

Triage, categorize and classify the incident, and decide on immediate containment measures

Perform a detailed assessment and formulate a specific plan of action, based on the type of incident

Containment

Example Activities

Deploy containment controls and monitor for effectiveness (configure IDS/IPS, block bad IP addresses, distribute or set Anti-Virus signatures on all systems, temporarily block the utilized network communication method, etc.)

Eradication

Example Activities

Identify and mitigate all vulnerabilities that were exploited

Return affected systems to normal operations

Perform on-going monitoring

Recovery

Example Activities

Confirm malware is eradicated

Restore data (if needed and possible)

Normalize affected networks

Lessons Learned

The Plan

We deliver a highly detailed **Cyber Incident Response Plan that provides much needed crisis management context** and guides the Response efforts within all relevant departments in the entire organization, and even outside of it. It also contains custom templates for rapid communications, forensics, auditing, reporting, escalation and much more.

Processes

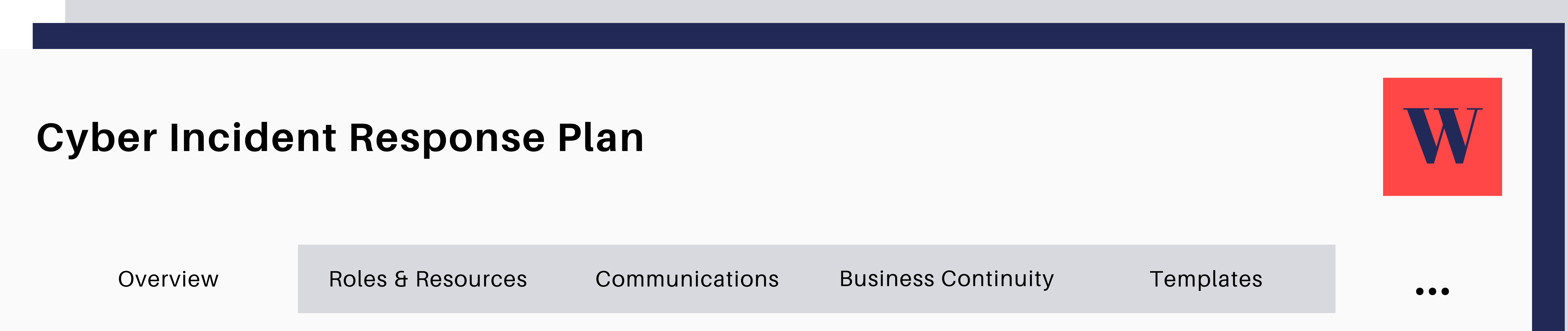
Detailed guidance on incident severity classification, correct playbook selection, escalations, communications, business continuity, 3rd party interactions, change and asset management and more across all 6 stages of the Response process

People

Cross-function collaboration is key during an incident; that is precisely why the Plan describes who, when and how performs which actions for maximum efficiency, as well as outlines each team's structure, RACI, backups, roles and interactions

Accelerators

Time and resources are everything in a crisis; we provide detailed plug-and-play templates and guidance for everything from reports, status tracking and email wording to contacts and law enforcement communications so you don't waste either



Cyber Incident Response Plan

The Playbooks

We use our expert knowledge of the cyber threat landscape and the results of a thorough risk assessment of your organization to create highly technical **Cyber Incident Response Playbooks - hands-on, detailed and specific to your very particular and unique business.**

Ransomware

DDoS Attack

Credential Theft

Malicious Insider

Privacy Breach

IoT Malware

Impersonation

Physical Breach

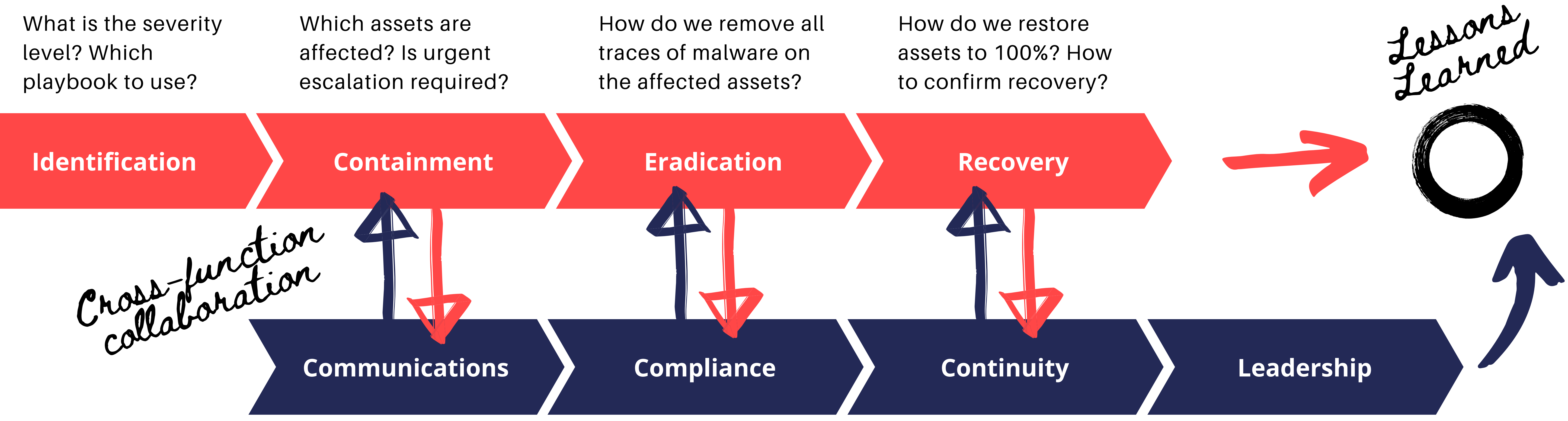
...

Each Playbook provides step-by-step guidance on how to resolve a specific cyber attack scenario most efficiently, minimizing stress, effort and losses across all stages of the Incident Response process:

1. **Preparation**
2. **Identification**
3. **Containment**
4. **Eradication**
5. **Recovery**
6. **Lessons Learned**

The Simulation ("Tabletop Exercise")*

We craft a bespoke cyber incident scenario unique to your organization and threats in your sector, and conduct a 4-6 hour cross-function simulation that requires actionable inputs from your **technical** (eg. cyber, IT) and **business** (HR, legal, executive) representatives at every step of the Incident Response lifecycle. When a real incident occurs, it'll be like riding a bike.



What is the severity level? Which playbook to use?

Which assets are affected? Is urgent escalation required?

How do we remove all traces of malware on the affected assets?

How do we restore assets to 100%? How to confirm recovery?

Identification

Containment

Eradication

Recovery

Communications

Compliance

Continuity

Leadership

Who needs to be involved and through which channels?

What is required from us to fulfill regulatory obligations?

How do we carry out normal business operations right now?

How do we maximize performance of everyone involved?

* This is a very simplified outline for display purposes, of course

What our clients say...

“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.”

Our Story

Wembley
Partners

Going to market since late 2019 and led by a global Board of industry professionals with over 160 years of expertise combined, Wembley Partners set out to become the world leader in Security Intelligence, Cyber Incident Management, and Assessment products and services for small to medium-size businesses. Recognized by NCSC as an Industry 100 company, Wembley Partners delivered over $280,000,000 in value to its clients in under 2 years.

17	Consultants with world-class certifications
62	Major clients, including Fortune 500

National Cyber Security Centre INDUSTRY 100

CYBER ESSENTIALS

Member CyberExchange

BETADEN

Thank you.

We look forward to working with you.

Americas

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

USA
Virtual Office
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