CYBERSECURITY™ UMBRELLA

Cyber Threat Awareness & Response Skills

TRAINING PARTNER

EC-Council

TECHNOLOGY PARTNER

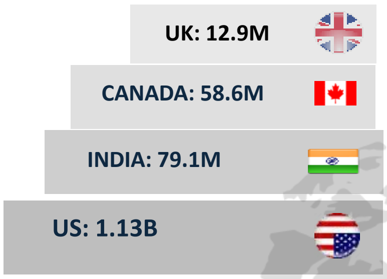
CERTIFIED PARTNER

TOP 10 GLOBAL THREATS

CYBERSECURITY UMBRELLA™
Cyber Threat Awareness & Response Skills

Our comprehensive research and analysis have identified the top 10 threats, shedding light on critical areas of concern within the current security landscape. These findings highlight potential risks and controls.

Top phishing targets



1. Phishing

Risks: Identity theft

Controls: Awareness training, Email filters

2. Insider Threats

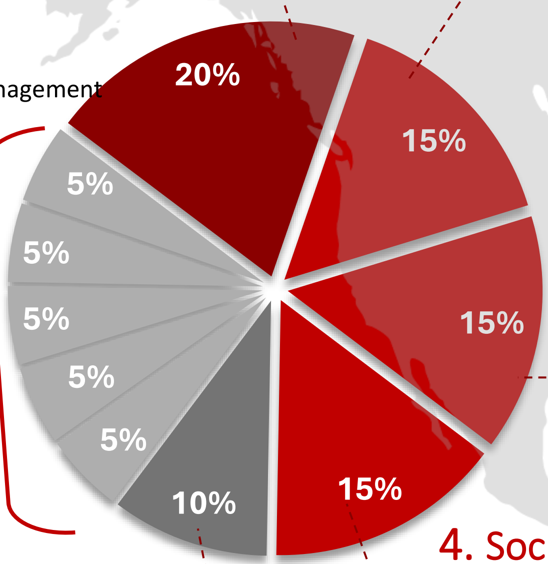
Risk: Data leaks, Sabotage, Fraud

Controls: Multi-factor authentication, least privileged principles, Data leakage prevention.

10. Backdoors

Risk: Data theft, unauthorized access

Controls: Monitor baseline asset management and change management.



09. Deepfake threats

Risk: Misinformation, erosion of trust.

Controls: User awareness training.

08. AI-Powered attacks

Risk: Weaker defence mechanisms.

Controls: Employ stronger algorithms.

07. Zero-day exploits

Risk: Service disruption, financial loss.

Controls: Segment network, Regular system patching update.

6. IOT Vulnerabilities

Risk: Unsecure communication, compromised devices.

Controls: Regularly update software.

62% involve ransomware or extortion, among incidents driven by financial motives.
$46,000 per breach (approx.)

3. Ransomware

Risk: Financial loss, Data loss, Denial of Service

Controls: Regular backups, system updates.

4. Social Engineering

Risk: Reputational damage.

Controls: User Awareness training.

68%
involved non-malicious human actions, like falling victim to social engineering or making errors.

5. Supply Chain Attack

Risk: Service disruptions, financial impact.

Controls: Vendor compliance.

Note: This data pertains to the year 2024.

SECURITY SERVICES OFFERING 1/3

CYBERSECURITY UMBRELLA™
Cyber Threat Awareness & Response Skills

We take a holistic view of our client's business priorities and create opportunities to address the risk to the most valuable business assets and implement an effective Cybersecurity Program to monitor and respond to threats.

1. PROFESSIONAL SERVICES & ASSESSMENTS

1.1. Vulnerability Scanning - we use a variety of tools and techniques to examine your information systems for security gaps and misconfigurations.

1.2. Penetration Testing - we simulate an attack on your information systems and applications. The focus of the penetration test is to determine what attackers can access and what damage they can potentially cause.

1.3. Web Application Assessments - this assessment focuses on a runtime analysis of your internet, intranet, and extranet web-based applications with the intent to expose weaknesses or vulnerabilities within your applications.

1.4. Wireless Network Vulnerability - Assessment - this premise assessment will reveal the security holes in your wireless infrastructure and provide consultation on how to remediate them.

1.5. Incident Post-Mortem Assessment - after an incident has taken place Cybersecurity Umbrella will give an analysis of why and how the incident happened. It is crucial for determining appropriate countermeasures to prevent a recurrence.

1.6. Policy & Procedures Design or Review - Cybersecurity Umbrella will determine whether existing policies are relevant or require updating based on established security standards such as ISO, ITIL, COBIT, etc.

1.7. Information Systems Audits - these audits will review and benchmark multiple areas of your organization to identify operational practices and systems configurations that represent a risk to your sensitive information.

1.8. Threats & Risk Assessments - Understanding and assessing risk is one of the most fundamental ways your organization can improve your information security decisions. A Cybersecurity Umbrella Risk Assessment formally documents the risks associated with your Information Systems and sensitive data assets based on the threats to the system and the vulnerability of the scheme to those threats and the potential impact of a security breach on the system. Risk assessments are conducted annually to account for changes in your operational environment.

1.9. Remediation Guidance - an assessment is just the first step towards enhancing your security posture. The all-important next step of remediating vulnerabilities often requires the
The high-level technical expertise of our professionals.

STATEMENT OF CONFIDENTIALITY:

THIS DOCUMENT AND SUPPORTING MATERIALS CONTAIN CONFIDENTIAL AND PROPRIETARY BUSINESS INFORMATION OF CYBERSECURITY UMBRELLA. THESE MATERIALS MAY BE PRINTED OR PHOTOCOPIED FOR USE IN EVALUATING OUR PROPOSED SERVICES BUT ARE NOT TO BE SHARED WITH OTHER PARTIES.

2. COMPLIANCE

Achieving compliance with industry standards does not have to be as complicated as it seems. Regardless of the norm, Cybersecurity Umbrella will guide you through the validation of conformity processes quickly and smoothly.

1.10. PCI DSS - Cybersecurity Umbrella consults with client organizations (merchants and service providers) that store, process or transmit payment card data. If your business falls into this category, we can ensure your business practices comply with the Payment Card Industry Data Security Standard (PCI DSS).

1.11. HIPAA, PHIPA or PIPEDA - health care institutions are required by law to protect the privacy of Protected Health Information (PHI), by the Health Insurance Portability and Accountability Act (HIPAA) in the United States. In Canada, the Personal Health Information Protection Act (PHIPA) and the Personal Information Protection and Electronic Documents Act (PIPEDA). Cybersecurity Umbrella will ensure your information systems and policies are compliant with these standards.

1.12. ISO or COBIT - clients who have adopted the framework of ISO/IEC 27002 (Code of practice for information security management) or Control Objectives for Information and Related Technology (COBIT), as a part of their overall Information Systems Risk Management and Security Policy Framework, look to us to help them continually verify compliance with these standards.

1.13. SANS Top 20 CSC - the SANS Top 20 Critical Security Controls (CSC) define and guide strategies for effective cyber defense solutions. It is a valuable checklist that Cybersecurity Umbrella uses to help security and IT managers evaluate how their systems and policies address major threats and vulnerabilities.

1.1. NIST or CSF - the “National Institute of Standards and Technology” (NIST) standards represent the pinnacle of cybersecurity excellence. NIST offers comprehensive frameworks like the NIST Cybersecurity Framework (CSF) and invaluable guidelines in Special Publications such as SP 800-53 and SP 800-171. These standards are the foundation of our cybersecurity strategy, aligning us with industry best practices and empowering us to effectively manage and mitigate cyber risks.

STATEMENT OF CONFIDENTIALITY:

THIS DOCUMENT AND SUPPORTING MATERIALS CONTAIN CONFIDENTIAL AND PROPRIETARY BUSINESS INFORMATION OF CYBERSECURITY UMBRELLA. THESE MATERIALS MAY BE PRINTED OR PHOTOCOPIED FOR USE IN EVALUATING OUR PROPOSED SERVICES BUT ARE NOT TO BE SHARED WITH OTHER PARTIES.

3. BEST PRACTICES REVIEW

Cybersecurity Umbrella's complete suite of managed security solutions takes care of everything you need to keep your data, email, website, networks, applications, and mobile devices safe and working for your organization.

1.14. Perimeter Network Security Device - Firewalls, IDS, and Web Filtering Devices are critical components of your enterprise network security infrastructure. A Perimeter Best Practices Review is performed to:

1.14.1. Use a relatively simple mechanism to significantly strengthen your organization's perimeter security and network segmentation

1.14.2. Verify that network segmentation, in fact, meets best practices and supports your business needs

1.15. Server Best Practices Review - allow us to safeguard your server and applications securely. We focus on the following:

1.15.1. Server configuration & Policy configuration Review using CIS/NIST Risk Practices

1.15.2. System & Device Hardening – eliminating as many security risks as possible, done by removing all non-essential rules/policies, whitelisting software programs, and services.

1.16. Mobile Security - Cybersecurity Umbrella offers a Mobile Security Management program that helps organizations build a risk management framework that is inclusive of mobile devices. Delivered by senior consultants with hands-on experience in security management and governance, the program evaluates your readiness for adopting mobile technology, with a managed and acceptable level of risk.

1.17. Technology Sourcing & Implementation - at Cybersecurity Umbrella, we partner with the top vendors in the security market to provide the hardware and software you need to keep your networks safe. You need a partner who can not only supply products but also helps you decide which technologies to purchase to meet your requirements best, which is where Cybersecurity Umbrella Security adds value.

PACKAGE OPTIONS

CYBERSECURITY UMBRELLA™
Cyber Threat Awareness & Response Skills

Our objective is to provide a suite of services that work best for your business environment.

SERVICES	500 Hrs.	500 Hrs.	600 Hrs.
Professional Services & Assessments on Demand			
Incident Post-Mortem Assessment	X		
Penetration Testing	X		
Mobile Application Assessments	X		
Network Vulnerability Assessment	X		
Wireless Vulnerability Assessment	X		
Configuration Best Practices Review		X	
Threats & Risk Assessments		X	
Information Systems Audits		X	
Policy & Procedures Design/Review		X	
Third Party audits		X	
Advisory and Remediation Guidance Packages			X
Security Assurance Report		X	
Compliance (Select at least one for the package)			
PCI DSS			X
PHIPA or PIPEDA			X
ISO or COBIT			X
SANS Top 20 CSC			X
Best Practices Review			
ERP, CRM, HIS, HRIS,			X
SIEM, DLP, IPS, Antivirus			X
Ransomware			X
Automation and BI			X

STATEMENT OF CONFIDENTIALITY:

THIS DOCUMENT AND SUPPORTING MATERIALS CONTAIN CONFIDENTIAL AND PROPRIETARY BUSINESS INFORMATION OF CYBERSECURITY UMBRELLA. THESE MATERIALS MAY BE PRINTED OR PHOTOCOPIED FOR USE IN EVALUATING OUR PROPOSED SERVICES BUT ARE NOT TO BE SHARED WITH OTHER PARTIES.

INTRODUCTORY OFFER

CYBERSECURITY UMBRELLA™

Cyber Threat Awareness & Response Skills

FREE HALF DAY SECURITY CONSULTATION

This free offer applies to new clients - consulting time is used towards any Cybersecurity Umbrella service. At the end of the allotted time, the client will receive a mini report of our findings. In good faith, the client also has no obligation to make any additional engagements with us.

A "half day" engagement is equivalent to four (4) hours of consultation.

STATEMENT OF CONFIDENTIALITY:

THIS DOCUMENT AND SUPPORTING MATERIALS CONTAIN AND PROPRIETARY BUSINESS INFORMATION OF CYBERSECURITY UMBRELLA. THESE MATERIALS MAY BE PRINTED OR PHOTOCOPIED FOR USE IN EVALUATING OUR PROPOSED ARE NOT TO BE SHARED WITH OTHER PARTIES.

CONTACT US

Canadian Address

1 Dundas St West, Suite 2500,
Toronto, ON, Canada, M5G 1Z3.

Web

www.cybersecurityumbrella.com

E-Mail

support@cybersecurityumbrella.com
research@cybersecurityumbrella.com

Telephone

Canada:
+1 (437)500-4213

Indian Address

3rd Floor, Above Central Bank of India, Opp. Mahalaxmi Juice,
Nr. Gujarat Gas Circle, Adajan Road,
Surat - 395009, Gujarat, India.

Web

www.cybersecurityumbrella.com

E-Mail

support@cybersecurityumbrella.com
research@cybersecurityumbrella.com

Telephone

India:
+91 709 602 2911
+91 261 355 4007

As the security industry saying goes, *"it is not about if you will be breached, it is about when".*

Per the Verizon report, you could breach right now and not know it. Allow us to help you evaluate your security posture and put your mind at ease.

STATEMENT OF CONFIDENTIALITY:

THIS DOCUMENT AND SUPPORTING MATERIALS CONTAIN CONFIDENTIAL AND PROPRIETARY BUSINESS INFORMATION OF CYBERSECURITY UMBRELLA. THESE MATERIALS MAY BE PRINTED OR PHOTOCOPIED FOR USE IN EVALUATING OUR PROPOSED SERVICES BUT ARE NOT TO BE SHARED WITH OTHER PARTIES.