Manipulating the Human Element: The Rise of Social Engineering in Cyber Crime

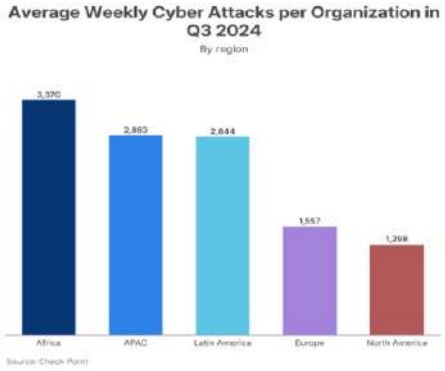
Saptarshi Chaudhuri – Head of Chedid Re Underwriting

Cyber attacks in 2024: Scale, Scope, and Sectors

By end-2025, global cybercrime costs are expected to reach USD 10.5 trillion, up from USD 3.0 trillion in 2015.[1] According to threat intelligence provider Cyble, Russia ranked as the country most targeted by cyber attacks in 2024, largely owing to geopolitical tensions, followed by Ukraine, the UK, and the US.

During the year, the global cybersecurity landscape was marked by a series of attacks that have impacted vital sectors, most notably[2]:

- **Healthcare:** Change Healthcare, a major US player in the healthcare sector, fell victim to a ransomware attack. The breach led to business interruptions and exposure of sensitive patient health (PHI) data, with nearly USD 22 million being paid in ransom.
- **Cloud Storage:** Snowflake, a prominent data warehousing company, experienced a significant data breach in mid-2024. Attackers exploited vulnerabilities to gain access to customer data, raising concerns about data security in cloud services.
- **Defence:** The UK's Ministry of Defence experienced a significant data breach involving PII (Personally Identifiable Information) of military personnel, after the payroll system of a contractor was attacked and compromised.
- **Telecommunications:** AT&T suffered two separate data breaches in 2024. The data of over 75 million customers was compromised and leaked into the dark web, raising massive security concerns.
- **Technology:** In May 2024, Dell confirmed a significant data breach, whereby cybercriminals accessed PII and financial information (PCI) of approximately 49 million customers.
- **Manufacturing**: In November 2024, Schneider Electric reported a major cyberattack, with hackers having stolen over 40 GB of critical data. This was the company's second breach of the year, highlighting the growing vulnerability and exposure of the manufacturing sector to cyber risks.
- **Information Broker:** National Public Data (NPD), a US data broker specializing in background checks, suffered a significant data breach in April 2024. The breach exposed 2.9 billion records with highly sensitive personal data of up to 170 million individuals across the US, the UK, and Canada.



- **Government Agencies:** In January 2024, an investigation concluded and reported that Russian hackers have targeted 65 Australian government departments and agencies, stealing 2.5 million documents. This alleged incident marked Australia's largest government cyberattack.

[1] Boardroom Cybersecurity Report 2023, Cybercrime Magazine

[2] Sources: Cyber Management Alliance, Bleeping Computer, Bloomberg Law

What is Social Engineering?

As cyber threats continue to evolve into the digital age, Social Engineering remains a favoured method for cybercriminals due to its effectiveness and simplicity. Rather than exploiting technical vulnerabilities of systems or software, it relies on the psychological manipulation of individuals. Social Engineering takes advantage of human emotions and impulses like trust, excitement, fear, or urgency, pushing people to disclose sensitive and/or confidential information – such as passwords, bank account details or access to restricted networks – they would not otherwise.

Common Types of Social Engineering Attacks[3]:

1. **Business Email Compromise (BEC):** A type of cybercrime where attackers manipulate or compromise legitimate business email accounts to request fraudulent changes to payment methods. These attacks generally target companies, organizations, or individuals in senior executive roles.

   BEC continues to evolve on the back of sophisticated targeting and social engineering, in the last 10 years, with these losses having recorded 17% year-over-year growth, according to the FBI (Federal Bureau of Investigation).

   The process typically involves the following steps:

   1. R**esearch**: information gathering about the target company and the target employee.
   2. **Contact with target**: establishing rapport and relationship to build trust with the target employee.
   3. **Exploitation**: manipulating the target employee into disclosing confidential information or performing a certain action such as sending a payment – usually posing as a senior exec to create a sense of urgency.
   4. **Execution and exit**: breaking contact and leaving no trace once the BEC attack is successfully accomplished without arousing suspicion.

2. **Phishing** – Attackers send fraudulent emails that appear to come from a trusted source, often trying to get the victim to click on a malicious link or attachment. In 2024, phishing attacks were responsible for more than 40% of Social Engineering cybersecurity incidents (Verizon).

3. **Vishing (voice phishing)** – Cybercriminals use phone calls to impersonate legitimate entities (like banks or government agencies) to extract personal information or money.

4. **Pretexting** – Attackers create a false sense of trust by pretending to need information for a seemingly valid reason, such as a fake job interview or a survey.

5. **Baiting** – Attackers offer something enticing, like free software or a prize, in exchange for private information or access.

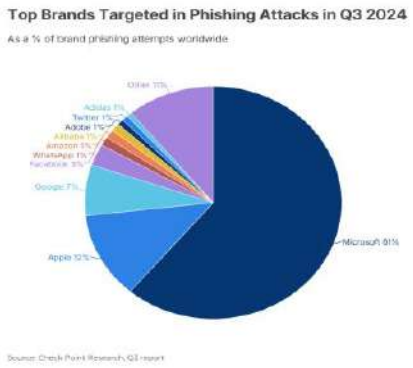
6. **Tailgating** – In-person Social Engineering where attackers gain physical access to a restricted area by following an authorized person through security doors.

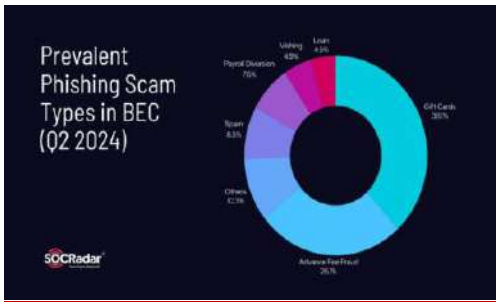
7. **Scareware –** A type of Social Engineering attack that is often used to convince individuals that their device is infected with a critical security issue, prompting them to take responsive action. Victims are encouraged to click on a button that is claimed to either remove the virus or download software that will uninstall the malicious code – with this button leading them to installing malicious software.

The widespread use of Artificial Intelligence (AI) tools such as Chat GPT has resulted in a paramount increase of Social Engineering attacks, especially phishing**.**

[3] Source for information on cyber-attack types: Crowdstrike

Chedid Re





The Impact on Corporations:

Social Engineering attacks can result in substantial financial harm. In addition to direct financial losses, these attacks can cause significant reputational damage that jeopardizes an organization's relationships and business dealings with its clients. They also raise considerable privacy concerns that can lead to regulatory and third-party claims exposure.

1. Financial Loss

- **Fraudulent Transfers:** Attacks involving fraudulent wire transfers, BEC, CEO fraud, the manipulation of banking details, or the issuance of payments to fictitious vendors can result in severe financial losses for the corporation.
- **Cost of Remediation:** Recovery from social engineering attacks involves substantial costs and expenses related to investigations, legal fees, incident response, and security upgrades. In some extreme cases, these costs can extend to hefty ransoms imposed by attackers on the corporation for it to regain access to sensitive data or systems.

2. Business Disruption:

- **Loss of Productivity:** Social engineering attacks can cause operational disruptions, leading to time-consuming and costly downtime that can severely impact the company's productivity and income potential.

3. Reputational Damage

- **Stakeholder Mistrust**: When customers, clients, or third-party vendors learn that an organization has been compromised, they may lose trust in its ability to safeguard their personal information.
- **Public Exposure**: High-profile social engineering attacks often receive negative media coverage and public scrutiny, both of which can greatly damage an organization's brand reputation.

4. Privacy Concerns

- **Data Breaches:** Stolen customer or organizational data can lead to significant privacy violations. This is especially concerning when this data involves Personally Identifiable Information (PII), Payment Card Industry (PCI) data, or Protected Health Information (PHI).
- **Identity Theft:** Stolen personal data can lead to lawsuits, customer complaints, and a growing perception that an organization is not equipped to protect sensitive information.

5. Regulatory and Legal Exposure

- **Regulatory Fines and Penalties**: In many sectors, regulators have put in place strict data protection and privacy laws (such as GDPR in the EU, HIPAA in the U.S., or the CCPA in California). If customer data is compromised in a social engineering attack, organizations may face regulatory fines for failing to meet these standards.
- **Compensation Claims**: Organizations are often contractually required to safeguard the data of their clients and partners. If an attack results in data loss or financial damage, these third parties can seek compensation for losses incurred because of the breach.
- **Litigation**: Customers can file lawsuits for negligence or failure to adequately protect their data, leading to costly and time-consuming legal cases.

6. Loss of Competitive Advantage

- **Intellectual Property Theft**: Social engineering attacks can lead to stealing intellectual property (IP) or sensitive business strategies, giving attackers access to trade secrets or valuable business information. This can affect an organization's competitive position and unique value proposition in the market.

Chedid Re

Prevention Strategies[4]:

1. Personnel:

- **Employee Training**: It is essential to provide regular and refresher training to employees with the knowledge to identify different forms of social engineering attacks such as phishing, pretexting, and baiting, among others.
- **Limited and considered online footprint**. The less individuals share information online and on social media, the harder it is for hackers to target them.
- **Simulated phishing campaigns**: Testing employees through simulated phishing attacks helps identify vulnerabilities and areas where they may need more training or awareness. HR (Human Resources) plays a critical role in this effort.
- **Incident reporting system**: A clear, simple, and anonymous method for reporting suspicious activity is crucial. Employees should feel encouraged to report incidents without prejudice or punishment.

2. Processes:

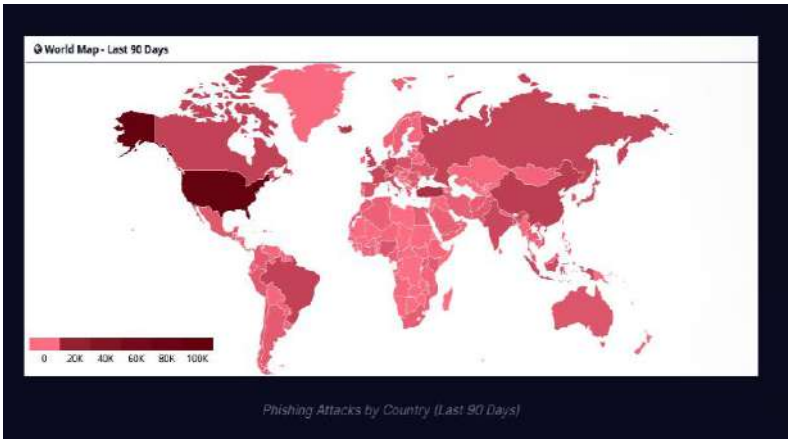
- **Policies and Enforcement**: Strong, clear policies for internet usage, protecting financial transactions, and safeguarding sensitive information should be put in place. Enforcement of these policies is key, as even the best policies are ineffective if not properly implemented.
- **Verification**: If someone contacts you claiming to be affiliated to a company or an organization, ask for proof of identity or contact the organization directly to verify the information.
- **Incident Response Plans**: A clear incident response plan that is regularly updated and tested ensures that the organization can react swiftly and appropriately when an attack occurs.
- **Regular security audits and assessments:** Mechanisms should be set up to make sure that plans and procedures are up to date and fit for purpose.

3. Technology:

- **Password Policies and MFA**: Enforcing complex passwords (e.g., a mix of characters, symbols, and length) and implementing multi-factor authentication (MFA) help prevent unauthorized access to sensitive systems. MFA, especially when tied to critical systems, significantly reduces the risk of attacks.
- **Install Antivirus Software/ Firewalls**: Must be installed and activated to keep devices protected at all times.
- **Data Backup**: Regular data backups are critical for recovery in case of ransomware attacks or other data loss incidents. Regular testing ensures the backups are reliable and functional.
- **Logging and Monitoring**: Implementing robust logging and monitoring systems is vital for detecting unusual or suspicious network activity. These logs can provide crucial information during post-incident investigations and help in the early detection of security threats.

4. Business Continuity Planning (BCP):

Last but not least, when an incident does occur, a robust Business Continuity Plan and Disaster Recovery plan are essential to ensure the organization can resume business as usual, as well as keep critical operations running during and after disruptive attacks and events



[4] Source for information on preventive strategies: Crowdstrike

Chedid Re

Social Engineering and Cyber Insurance:

As social engineering attacks grow more sophisticated, organizations are adjusting their risk management strategies, with greater emphasis on tailored and comprehensive insurance coverage. The sophistication of social engineering attacks has led to an evolution of cyber coverage that goes beyond traditional cyber risks – like data breaches and ransomware attacks – and that addresses emerging risks, particularly the rise of impersonation fraud and physical property loss. Below is a closer look at how these areas are evolving:

1. Impersonation Fraud

This coverage protects against attacks where fraudsters pose as the insured or their clients to divert funds, often without any prior system breach. These attacks can target organizations through emails or phone calls, making them harder to detect. While insurers can offer this coverage, some policies offer sub-limited protection against these emerging risks, especially in comparison to more traditional cyber risks like data breaches.

2. Physical Property Loss

Historically, cyber insurance covered financial losses resulting from data breaches or system failures. However, with the rise of social engineering, insurers have started to include loss of physical property. There are instances where attackers impersonate a legitimate company representative to authorize shipments or inventory orders. Given the potential impact on business operations, some policies are expanding their coverage to include these types of losses as optional or standard Endorsements.

3. Cyber and Crime Insurance

Both cyber insurance and crime insurance coverage need to be tailored to address newer forms of fraud, such as deepfake AI and impersonation scams. These types of attacks are more difficult to detect, and traditional policies may not provide adequate coverage for such losses.

Summary:

Social engineering attacks pose a significant and increasing threat to security. As these attacks evolve, prioritizing human-centric information security is essential. To mitigate risks, organizations must adopt a proactive approach that includes regular cyber awareness training and workshops; improved network security; multi-factor authentication (MFA), frequent security assessments and penetration testing; and robust Business Continuity Planning (BCP) ahead of attacks. Looking ahead, the rise of AI and machine learning will likely lead to more sophisticated social engineering attacks, making it crucial for the cyber security apparatus to stay one step ahead of the curve.

Working with a Specialist Broker

The above cases highlight the importance of working with a specialized insurance broker who can navigate the complexities of cyber risks and cover. Specialized brokers can offer solutions that not only provide the necessary protection for an organization, but also consider the affordability of premiums. Cyber insurance policy wordings can vary significantly in terms of language and coverage scope, and programs can be tailored to meet the client's specific needs. Additionally, some cyber insurance providers offer both pre-incident and post-incident protection, along with incident response solutions, including public relations and crisis management. It is essential that your broker takes all these factors into account, ensuring peace of mind and technical support when needed.

Chedid Re:

Chedid Re specializes in providing targeted cyber reinsurance brokerage solutions across key sectors that are critically vulnerable to digital threats – including banking, hospitality, healthcare, insurance brokerage, and consultancy. Leveraging an expansive network of over 400 employees in strategic global hubs and emerging markets – covering Europe, the Middle East, Africa, and South Asia – Chedid Re is uniquely positioned to deliver cross-border cyber risk solutions.

Supported by the robust infrastructure of its parent investment group, Chedid Capital, Chedid Re's reinsurance capabilities and risk management solutions enable its partners to build resilience, safeguard their financial stability, and scale their growth ambitions in the digital economy.