SECURANCE CONSULTING
Advantage of Insight | AI

# Humans vs. Security: The War on Social Engineering

www.securanceconsulting.com

# INTRODUCTION

No one likes to get duped. Egos are bruised, trust is lost, and coworkers and management can be hasty to point fingers. This is often the aftermath of a social engineering attack, when even well-meaning employees fall victim to hacking techniques poised to steal confidential information. Evolving with the times— and the hackers— is sometimes perceived as time consuming, costly, and, for some executives, unnecessary. However, the fact remains that the average cost of a data breach in the U.S. was **$8.64 million** in 2019[1], with social engineering attacks accounting for **67 percent** of all breaches.[2]

**How do we safeguard our finances and data, given the alarming statistics?**
More importantly, how do we get the entire organization on board, so our efforts to increase security awareness are not squandered? It starts with understanding what social engineering actually is. Only after knowing an enemy's strategies can one hope to defeat them.

# WHAT IS SOCIAL ENGINEERING EXACTLY?

If you receive an email from a Nigerian prince asking for a loan now in exchange for riches beyond your wildest dreams later, you are the target of social engineering. The hacker's objective is to circumvent security by attacking the weakest element: humans.

As employees, we have access to data that could compromise our employer, and we can be tricked in ways a computer cannot. Social engineers use our humanity against us, appealing to our sympathy, intelligence, and egos, to elicit information they may later use to infiltrate the company network.

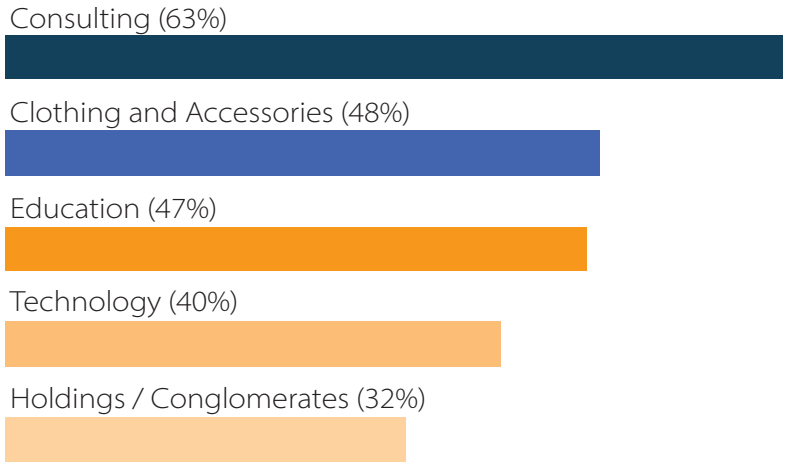
Put simply, social engineering is an attack vector, a method of manipulating and exploiting the human element to bypass physical or technical security controls. A hacker might not be able to walk in through the front door alone, but if he convinces someone on the inside to unlock it, it doesn't matter what kind of defenses are in place.

> The average time to identify and contain a breach is 280 days.[1]

# TACTICS AND TARGETS

If a social engineer approaches you with an objective in mind, be ready for an array of tactics. The common thread here is deception. Whether by email, in person, or on the phone, the hacker's intent is to draw you in, gain your trust, and abuse your knowledge or privileges.

## Top 5 sectors with the highest click rates on malicious links in phishing emails




*2020 Phishing Trends Report, Keepnet Labs, 2020*[3]

# HOW THEY GET US

**Phishing**— By far the most common social engineering attack vector, phishing involves emails that entice the target to click a URL or embedded link that appears legitimate. In fact, these links lead to fake websites or forms soliciting sensitive information, including login credentials, company financials, and names, addresses, and social security numbers, collectively known as personally identifiable information (PII). While they are numerous, phishing attacks are usually easy to identify by their suspicious grammar, spelling errors, and vague content.

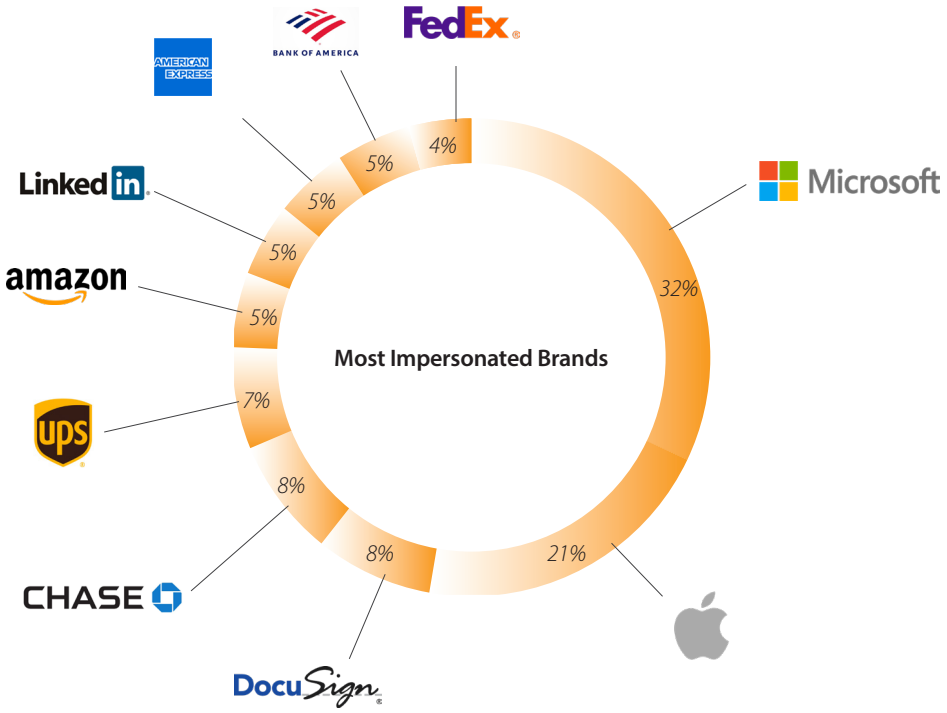
**Spear phishing**— A more targeted form of phishing, spear phishing emails focus on a specific organization or individuals within that organization. Rather than casting out a net and hoping for a catch, hackers spend months obtaining information about their targets in order to sound believable when the time comes to attack. For instance, hackers may send emails using a coworker's name or manipulate the SMTP mail header to look like it's coming from the company domain.

**Phone pretexting**— This type of social engineering is not about hacking via SMS. Instead, "pretexting" indicates the malicious outsider is fabricating a scenario (the pretext) to influence the target insider. Usually, the hacker already knows pieces of sensitive information, such as date of birth, a billing address, or even a mother's maiden name, and continues to build upon the lie to get what she wants.

**Dumpster diving**— Yes, they will. If a hacker thinks he has something to gain, dumpster diving won't be below him. Most of us toss junk mail and papers we no longer need into the garbage without a second thought. Company organizational charts, policies and procedures, phone charts, letterhead, and hard disks can all fall into the wrong hands, simply because someone is— literally— willing to take the leap.

**Tailgating**— You won't be celebrating with pizza and friends if a hacker pulls off this technique. For those who are adamant about gaining physical access to a facility, there is no shame in slipping through a door after an authorized employee makes her way in.

**Baiting**— If a hacker gains entry to a facility, he may leave behind a nasty surprise in the form of a seemingly harmless USB. Unsuspecting and well-meaning employees are expected to pick up the abandoned media and plug it into a computer, releasing malware onto the company's network.




*2020 Phishing Trends Report, Keepnet Labs, 2020*[3]

# CHALLENGES AND IMPACTS

Social engineering attacks present challenges to every industry at every level, from HR to IT, to the C-suite. A lack of internal guidance, security training, proper testing, or a security awareness plan with documented policies and procedures leads to unprepared employees and an improved success rate for social engineers. Despite the hurdles an organization might encounter, the long-term consequences of not implementing defenses against social engineering attacks can prove more costly than investing time, money, and resources in preparation and countermeasures.

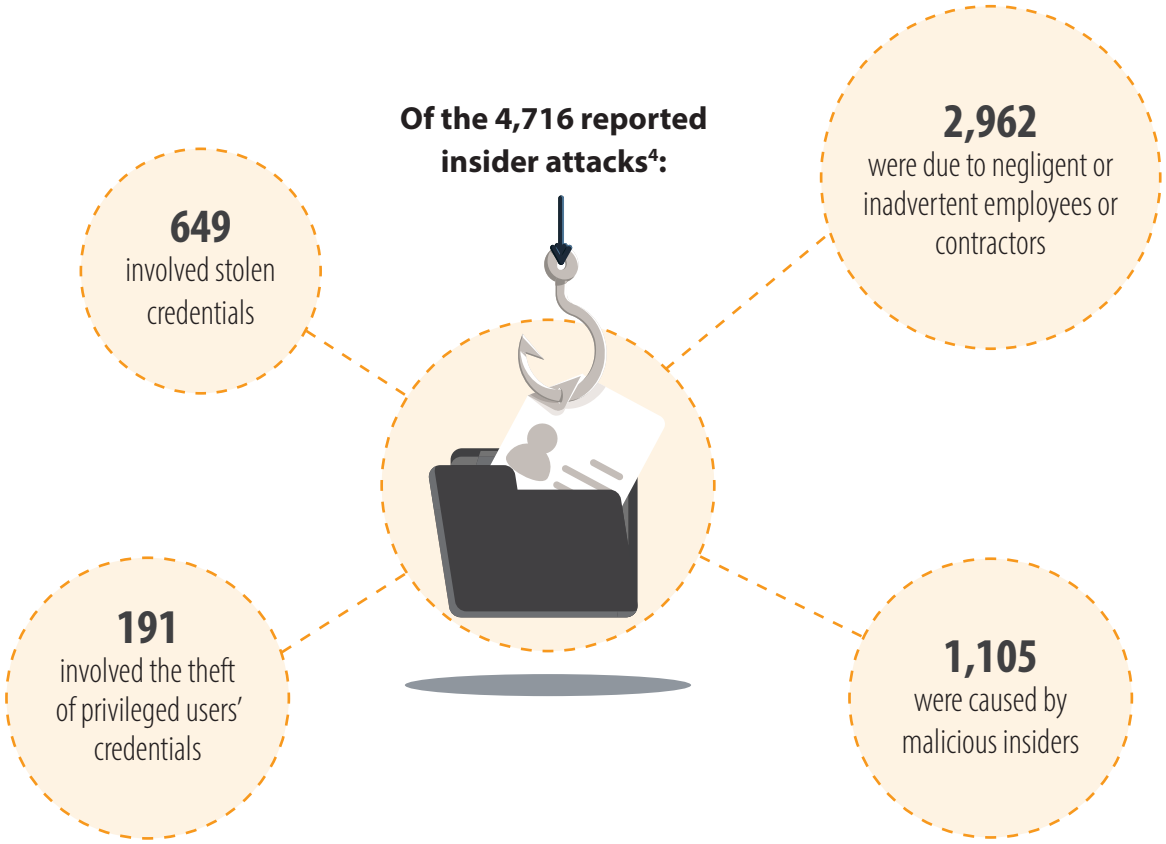
### Internal Hurdles

Every business operates on a budget, and the keepers of those budgets (read: C-level executives) aren't always on board when it comes to establishing a proactive approach to thwarting social engineers. Most funding is spent on the technical aspects of security, with little, if any, left for the human element (arguably, the weakest link). Traditional decision makers still rely on firewalls, permission controls, and patches to keep their networks safe, rather than integrate social awareness training or update policies and procedures to reflect best practices. This stagnant mode of thinking must evolve if organizations hope to stall the rise of security breaches perpetuated by hackers today.

> The average global cost of a data breach is **$3.86 million**.[1]

### Insider Threats and Privilege Abuse

It's not easy to detect an attacker who's inside your network— much less one who is allowed to be there. Since 2018, the number of insider threats has increased **47 percent**, from 3,200 in 2018 to **4,716** in 2020.[4] Traditional targets of malicious insiders include PII, electronic (or hardcopy) protected health information (ePHI), trade secrets, financial information, and even criminal history. As for their motives, financial gain is the undisputed leader, while some simply can't control their curiosity. Others are looking for information that will give them a competitive edge in their careers.




### Weak or Nonexistent Security Awareness

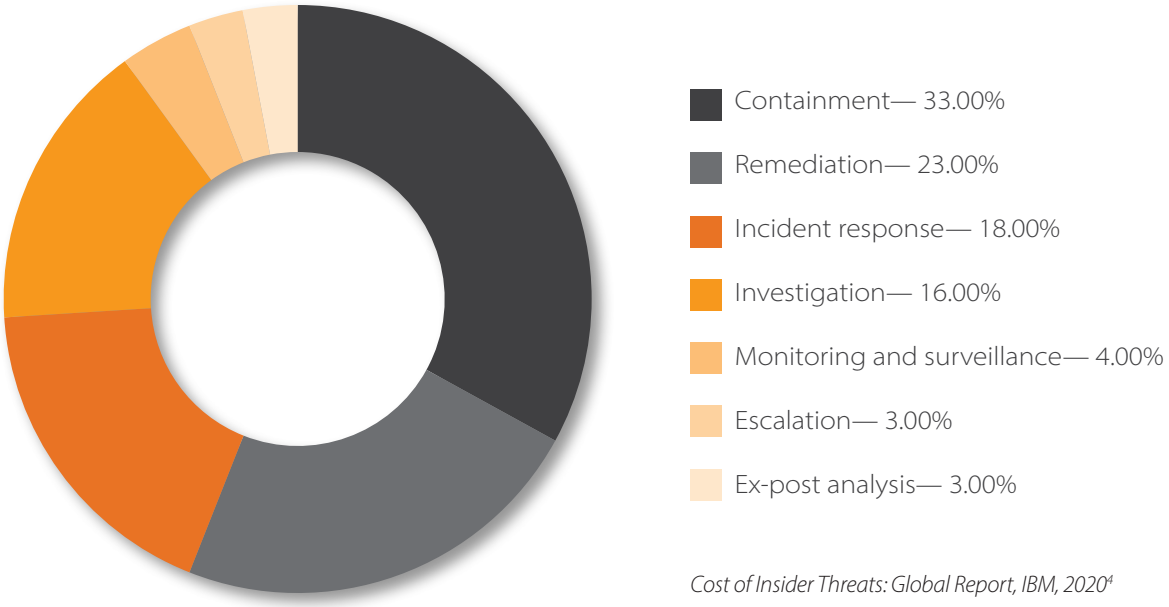
Employees can't fight threats they don't see. If higher-ups in the organization do not emphasize security awareness and put a training plan in place, the people who work for them will remain ignorant of how to combat malicious attacks. Keep in mind that social engineers' goals may involve remaining inconspicuous, and overwhelming charm often leads them to success. An employee may leave her encounter with a social engineer none the wiser that she's compromised the business. In fact, she might even think that she's done a good deed.

> The average global cost of insider-related incidents has increased 31 percent— from **$8.76M** in 2018 to **$11.45M** in 2020.[4]

### Financial Loss

More than **$26 billion** was stolen globally from small to large companies between 2016 and 2019 due to business email compromise (BEC), according to the FBI.[5] This figure includes 166,349 separate incidents, which were reported across all 50 states and 177 countries. In 2019, the FBI received approximately 24,000 complaints about BEC scams, with a total loss of $1.7 billion and an average loss of roughly $72,000.[6]

## Percentage Costs of Insider Threats By Phase




*Cost of Insider Threats: Global Report, IBM, 2020*[4]

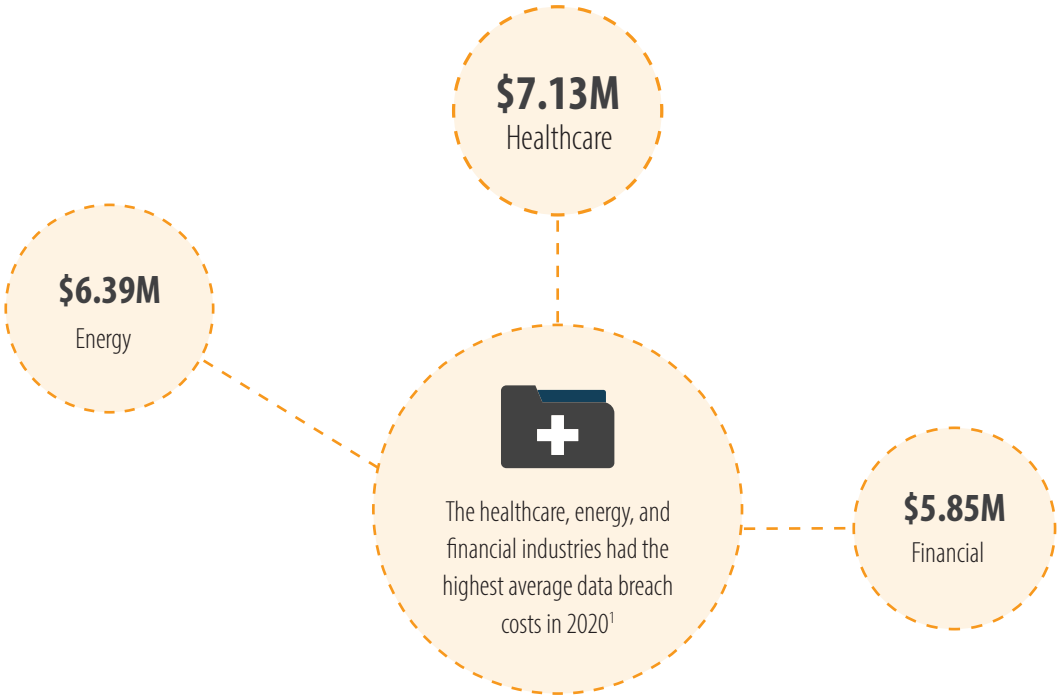
# STOP HACKERS IN THEIR TRACKS

As we mentioned before, humans are fallible. That's what social engineers count on. That said, there are precautions organizations can take to safeguard data, educate employees, and improve overall security posture to thwart ne'er-do-wells in their pursuit of protected information.

### Testing

Any strategy must be tested rigorously if it is to effectively accomplish its goals. Simply checking the boxes when it comes to security gives malicious attackers the upper hand. Organizations should test the effectiveness of user security awareness training as proactively as they do traditional security defenses. Social engineering simulations, which are easy to perform in a business setting, include mock phishing, baiting, tailgating, and phone pretexting. These assessments can be performed discreetly, so employees are none the wiser, and the results truly capture the current state of user awareness. Keep in mind the goal is to educate, not to shame employees for taking the bait.

Social engineering tests can also help organizations identify technical vulnerabilities, such as email, DNS, and web server configuration flaws, which might require hardening to decrease the probability of malicious insiders' requests reaching other employees. While these assessments must be performed in a live environment, they do not necessarily have to disrupt the normal workday or result in lost productivity.




**Policies and Procedures**

Formal policies and procedures are a must for an effective security strategy. These documents spell out the organization's intent, scope of concern, and exact standards when it comes to its response to social engineering. Policies should cover all facets of security, including personnel, physical security, and network and system technologies. Employees should be able to easily consult these policies for guidance on how to identify and ensure the protection of sensitive information, maintain strong passwords, defend against malware, and stay up to date with countermeasures for hacking techniques they might be exposed to. Policies and procedures should be reinforced with continuous social awareness education.

**Social Awareness**

Social, or security, awareness is necessary for every person who uses the corporate network. It isn't enough to document policies and procedures; employees have to live them. Building awareness must become a culture.

Employees should be made aware of existing policies and procedures, the incident response plan, and the damage that can be wrought by a successful breach. Sharing real examples of companies hacked via social engineering will place tangible consequences in employees' minds about the harm one incident can cause.

> Incident response preparedness saved businesses an average of $2M in the event of a data breach.[1]

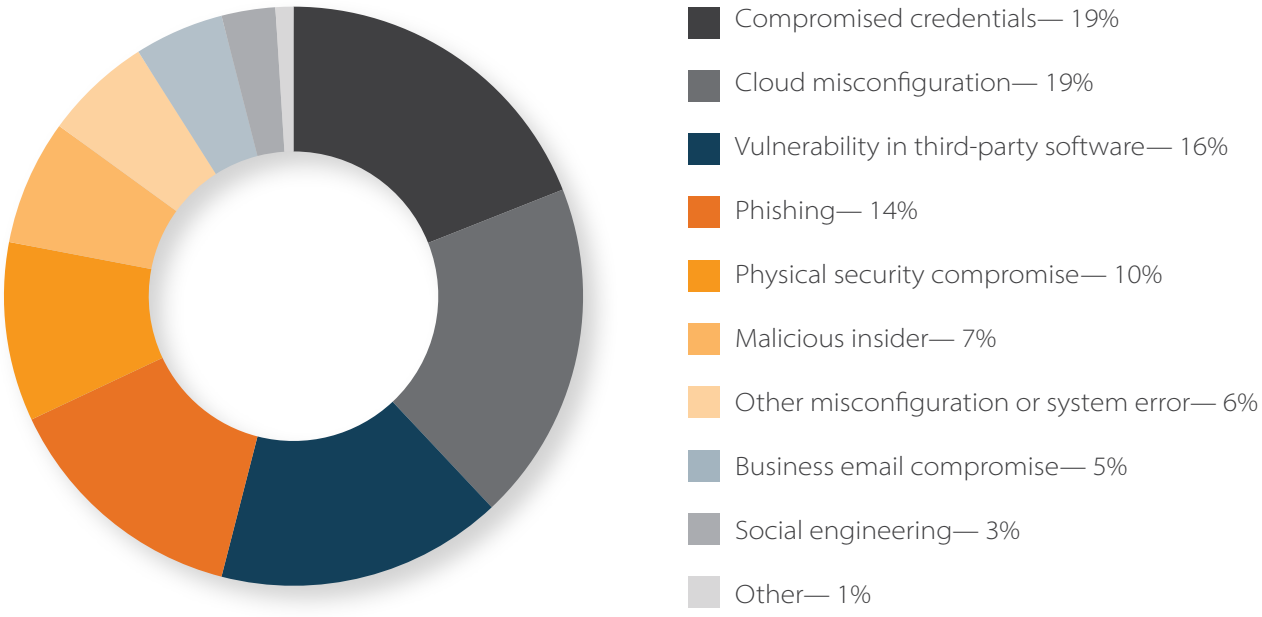
## Important Policies and Procedures

- **Computer system usage**
- **Information classification and handling**
- **Personnel security**
- **Physical security**
- **Information access**
- **Virus protection**
- **Information security awareness training and compliance**
- **Compliance monitoring**
- **Password policies**
- **Retention and destruction of documentation**

### Security Incident Management

A solid security incident management plan will help put out fires before they engulf the business. When an incident occurs, each department should know its role in informing customers or business partners and in the remediation process. Because security breaches can lead to substantial financial or data loss, security, IT, and legal teams will need to collaborate quickly to notify affected parties and protect the business from further attacks. The U.S. Secret Service, which has released several cybersecurity trainings, encourages the development of a cybersecurity incident response plan, involving specialized legal counsel, expert third-party incident response organizations, and law enforcement.[7]

## Data Breach Root Causes




*Cost of a Data Breach Report, IBM, 2020*

# CONCLUSION

Social engineering techniques are evolving. Malicious actors are gutsy, charming, and have no shame when it comes to tricking helpful employees into revealing an organization's sensitive information. The best defense against their schemes is developing a security-aware culture by continually updating policies and procedures, involving all departments in the education and response phases, and conducting rigorous, scheduled testing of the human element of security.

Providing examples of successful attacks can motivate decision makers to give a green light to security initiatives, as well. In a world where numbers are everything, nobody wants to be a statistic. If your internal audit or IT department is not equipped to perform testing, consider hiring a third-party consultant to develop and execute an assessment plan that fits your organization and budget.

**Contact Securance to learn more about how your organization can safeguard finances, protect sensitive information, and win the war on social engineering.**

# ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

# SOURCES


[1] https://www.ibm.com/security/data-breach

[2] https://enterprise.verizon.com/resources/reports/dbir/

[3] https://www.keepnetlabs.com/2020-phishing-trends-report/

[4] https://www.ibm.com/downloads/cas/LQZ4RONE

[5] https://www.ic3.gov/media/2019/190910.aspx

[6] https://pdf.ic3.gov/2019_IC3Report.pdf

[7] https://www.hsdl.org/?view&did=763317


*Human Vs. Security: The War on Social Engineering*


*© 2020 Securance LLC. All Rights Reserved.*



SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102,Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com