Courtesy of
THIA

CYBERRISKS&LIABILITIES

Hacktivism Explained

Hackers exploit virtual vulnerabilities to gain access to networks and devices illegally. While most engage in this activity for financial gain, others, called hacktivists, have different motivations. These threat actors typically engage in disruptive or damaging virtual activity on behalf of a political, social or religious cause. Individual or group hacktivists often work to expose fraud, reveal corporate wrongdoing or greed, draw attention to human rights violations, protest censorship or highlight other social injustices.

To spread their messages, hacktivists engage in various tactics, such as leaking sensitive data about and/or belonging to organizations, defacing web pages and taking organizations offline. Hacktivists often target government agencies, multinational corporations and powerful individuals to expose a believed injustice. The following are some of the motivating factors of hacktivism:

- **Political**—This motivation drives malicious actors to promote or upheave a political agenda.
- **Social**—This motive causes threat actors to shed light on social injustices.
- **Religious**—This motivation spurs hacktivists to discredit or promote a religious ideology.
- **Anarchist**—This motive inspires malicious actors to cause social distress by hacking entire populations.

Types of Attacks

While activism is a protected activity, hacking is not. Though hacktivists may have noble intentions, hacktivism is still categorized as cybercrime and is illegal regardless of motivation or outcome. In fact, hacktivists often employ the same tools and tactics as typical hackers. Some common types of attacks include:

- **Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks**—Usually targeting large organizations, DoS and DDoS attacks shut down machines or networks by flooding them with false requests and making them inaccessible to their intended users.
- **Doxing**—This tactic leaks confidential information of public figures, organizations or government bodies to the public.
- **Defacement**—Hacktivists utilize defacement to alter the appearance of a website, typically to spread activist agendas on government websites.
- **Data theft**—Hacktivists can steal data, intellectual property or other proprietary information.

Preventing Hacktivist Attacks

Since hacktivism aims to draw attention to a cause, hacktivists often reveal their targets and intentions in advance to gain attention, recruit new supporters or help fund their endeavors. Because financial gain is not the goal, any company of any size could be at risk of such attacks and face service disruptions, financial losses, data theft or reputational harm. The following are ways to combat hacktivist attacks:

- **Train all employees on cybersecurity best practices.** According to the IBM Cyber Security Intelligence Index Report, 95% of cybersecurity breaches are primarily caused by human error. Therefore, organizations need to teach their

Ted Hamm
INSURANCE AGENCY

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.