BINARY DEFENSE™ | 2019 White Paper

YOUR BUSINESS HAS MORE THAN HACKERS TO WORRY ABOUT

Protect Against Physical, Cyber, and Reputational Threats

Introduction: Threats to Your Business Take Many Forms Today

With breaches making the news on an almost daily basis, no business can afford to let down its guard when it comes to protecting its business systems, customer data, intellectual property, and other digital assets from cyberthreats. However, the threats don't end there.

In fact, companies must be prepared for other potentially catastrophic threats, vulnerabilities, and risks—everything from disgruntled employees attempting to sabotage the business to angry customers threatening employees, from industrial spies trying to gain access to your facilities to competitors slandering your business on social media. Any of these threats, if successful, could inflict serious financial, reputational, and/or human loss to your business.

While physical and reputational threats aren't necessarily new, they have changed substantially in the context of the technological society we now live in. Is your business prepared for a violent threat that emerges on social media and culminates at one of your locations? Can you combine intelligence across physical and digital environments to catch threats of all types before they are acted upon?

Today's threat landscape requires that you have a holistic approach to the threats against your business or organization. To do this, you need a proactive counterintelligence resource that provides a combined physical and information security (infosec) perspective to your IT and security, legal, human resources, marketing, and executive teams.

Growing Workplace Threats 48%

48% of U.S. human resources professionals report that their organization has experienced an incident of workplace violence.

Source: "Workplace Violence: A Growing Threat, or Growing in Awareness," Society of Human Resource Management (SHRM), March 2019

Adapting to the New Reality of Business Threats

Consider the following scenarios and whether your business would be prepared to quickly identify and thwart any of these situations before they develop into something more serious:

A new employee takes selfies while at your customers’ locations or homes and posts them on social media, identifying your business and potentially exposing private or damaging information about your customers.

A former employee makes threats in an online forum against his former boss at your company and voices plans to show up at your office to follow through on them.

A hacker group posts a list of targeted businesses for distributed denial of service (DDoS) attacks and your business is a stated target.

These are only a few examples of the many different forms that threats can take, both online, offline, and, increasingly—a blend of both.

For certain industries or types of organizations, additional types of threats can come from individuals or groups whose motivations go beyond the typical money, power, or retribution intentions. These threats may be unique to your particular business or organization based on its religious or political activities or affiliations, types of products it manufactures or sells, or unique characteristics of your customer base or geographical location.

Connecting the Dots Between the Real World and the Digital One

No matter the industry or company size, organizations need a holistic security approach that can connect online events, indicators, and data with real-world intelligence to identify threats to digital, physical, and reputational security. This requires an overarching approach to threat intelligence and security. For instance, the human resources (HR) department shouldn't have to work on its own to handle unhappy or former employees. Instead, HR should be working hand-in-hand with intelligence experts who can monitor situations for indicators of threats.

There are many other examples of specific departments or functions that need to work collaboratively with intelligence experts to accurately and quickly identify threats and risks and take appropriate action to protect the company. See Table 1 for examples of departments and the threats they may need to identify and protect against.

Business Function	Potential Threats to Identify
Social media team	Monitor social media for negative comments, threats, and hackers
Marketing team	Monitor websites and other forums for negative comments, slander, and other reputational risks to the brand, as well as threats and hackers. Get insights into competitor products and solutions as well as customers and trends
IT/Infosec team	Discover compromised assets and sensitive data, intellectual property, and other digital assets that have been exfiltrated
Physcial security team	Monitor for unusual/abnormal employee and customer behavior
HR	Identify sexual harassment. Monitor for threats or negative comments from disgruntled or former employees
Executives	Identify threats to personal safety or reputation
Legal	Identify license infringement or theft of intellectual property
Software Development	Monitor for developers uploading code (with or without malicious intent) to public Github sites to identify potential exposure/loss of intellectual property

Figure 1. Threats and the Parts of the Business Involved in Identifying Them

Taking a Holistic Approach With Counterintelligence

Creating an effective program that protects against the threats to today's businesses and organizations requires a combination of skilled and experienced security professionals and sophisticated technology working in the form of a counterintelligence team. To be effective, the team must have awareness and insight into both: 1) The general threats emerging from hackers, hacktivists, state-funded bad actors, and other cybercriminals; and 2) The types of threats, vulnerabilities, and risks for a specific industry, business, or organization.

The team must also be able to identify and recommend action to protect against multiple types of threats and threat indicators, including, but not limited to:

- **Slander**
- **Menacing**
- **Compromised assets**
- **Theft**
- **Disgruntled employees**
- **Physical threats to employees**
- **Brand image**
- **Bomb threats**
- **Fraud**
- **Protests**

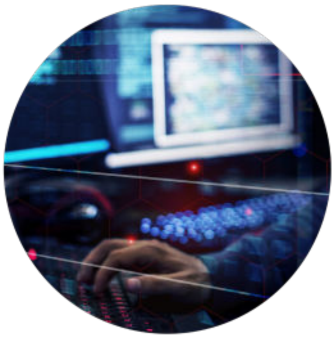
The challenge for most companies is that they don't have the internal resources, unique skill set, or budget it takes to operate a mature counterintelligence center. Instead, some try to make do with off-the-shelf threat intelligence reports and raw data about cyberthreats. The problem with this approach is that without a broader scope of inteligence combined with skilled security specialists, it's difficult, if not impossible, to connect all the dots accurately and quickly, both online and offline.

For this reason, many companies and organizations are turning to expert, third-party services to deliver the comprehensive counterintelligence and protection they need for their business.

Choosing the Best Counterintelligence Service

A credible, effective counterintelligence service should identify online, offline and blended threats to an organization so that it can better protect against malicious activity, no matter where it originates. This requires going far beyond commoditized threat databases and reports to uncover and analyze intelligence and indicators from the Internet (clear net), social media, the Darknet, and other sources.

Basic threat intelligence services don't deliver all the capabilities, skills, and technologies your business or organization needs for comprehensive counterintelligence and protection. To weed out these more limited services from a true counterintelligence operation, look for the following:



Technology

The counterintelligence service should use advanced and automated technologies, techniques, and applications to automatically search and alert on threat indicators as well as sensitive information on the dark net, Internet, and social media.

Expertise

Members of the CI team should be experienced information security and security professionals, with relevant backgrounds. Intelligence specialists & security researchers should have specialized skills appropriate to different types of threats.

Process & Communication

To serve as an effective early-warning system, the counterintelligence team needs to correlate, validate, and analyze threat information, determine the level of threat, and deliver actionable threat intelligence with context to your business.

Breadth of Depth of Intelligence

This service should provide your business with global reach, going beyond simply tracking common threats by deploying techniques such as infiltrating threat actor groups in the dark net to cultivate specific insight. It should be custom-tailored to your interests and specific risks, with the ability to monitor for them across potential threats.

Conclusion

Threats today come in all shapes and sizes, making it extremely challenging for your business to anticipate, identify, and pre-empt them. A counterintelligence service is the best way to gain a complete perspective across the physical and digital landscape to help you protect your business, employees, executives, and customers from harm.

Binary Defense Counterintelligence delivers the technology, expertise, processes, communication, and depth and breadth of intelligence you need to be prepared whenever and wherever threats arise. Our expert Counterintelligence Team proactively uncovers and analyzes intelligence from the Internet, social media, Darknet and other sources to identify threats to your organization, including potential attacks against key members and VIPs. We also keep our finger on the pulse of global security, providing you with actionable insight related to physical and public image threats. Finally, we incorporate our counterintelligence insights into other Binary Defense solutions to improve security for all of our clients against the latest attack types.

To find out more about how Binary Defense Counterintelligence can help protect your business, visit BinaryDefense.com/CI.

About Binary Defense

Binary Defense is the full-service security partner—real people, detecting real threats, in real time—and a global leader in advanced managed security solutions. Serving as an extension of your internal security and teams, Binary Defense offers world-class expertise and industry-leading, technology-agnostic security solutions including: Managed Detection & Response, Managed Security Information and Event Management (SIEM), Security Operations Center (SOC)-as-a-Service, and advanced Counterintelligence services. Built, tested, and constantly improved upon by top security researchers and hackers with the focus of detecting and protecting against next-generation threats, Binary Defense's cybersecurity solutions improve your organization's security posture today and into the future.

600 ALPHA PARKWAY, STOW OH 44224 | 800-BINARY2

WWW.BINARYDEFENSE.COM