proofpoint.

PROTECTING YOUR EXECS AND OFFICES

EXECUTIVE AND LOCATION THREAT MONITORING

A company's executives and physical assets have become focal points for unhappy customers, activist groups, cyber criminals, and even disgruntled employees who want to do harm.

While your executives focus their attention on growing the business, a hotbed of security-risk chatter on social media and the deep, dark, and surface web can pose significant risks to them, as well as your office locations. In fact, 84% of top 25 Fortune 500 CEOs were victims of threats and hate speech on Twitter and the dark web in February 2018.

While the threats and associated risks vary, they are all complex to mitigate without visibility. As part of your organization's cyber threat intelligence, it's crucial to monitor the social media and web spheres to gain visibility into all relevant threats to your key employees and locations.

> 84% OF TOP 25 FORTUNE 500 CEOS WERE VICTIMS OF THREATS AND HATE SPEECH ON TWITTER AND THE DARK WEB IN FEBRUARY 2018.
>
> – Proofpoint Research

THREATS TO YOUR EXECUTIVES

Executives in all industries are attractive targets for a range of threats—from verbal to physical attacks. Protecting your executives requires monitoring the digital universe for posts and conversations that present a risk.

Threats to physical wellbeing

From business and vacation travel to social media activity and more, there are a number of ways an executive can be tracked and eventually attacked. Cyberstalking, intimidation, and direct threats to your executives can deeply impact their sense of safety and wellbeing.

These threats are rampant on social networks, like Twitter and Reddit forums, and in the deep and dark web where users need a Tor browser to access nonindexed onion sites. Given the "promise of anonymity" inherent in the dark web, bad actors expect that their targets won't detect and monitor these conversations.

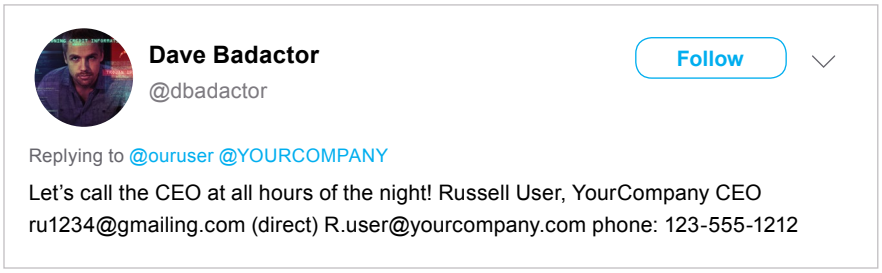
Doxing

We've seen doxing used in politics and to expose celebrities. When it comes to organizations and your executives, doxing usually takes the form of harassment and blackmail. Think back to the 32GBs hackers published, exposing personal details on its entire customer base, when Ashley Madison refused to pay the demanded bitcoin ransom.

Doxing can happen anywhere, including Pastebin where bad actors can broadly and publicly publish information about key executives to a wide audience. Once your executives' details are posted in a public arena, they can then be threatened publicly or privately by anyone who wants to harass or harm them.

Account compromise

Targeted cybersecurity threats represent one of the greatest challenges to information security. Gaining access to your executives' privileged credentials (dubbed "the keys to the kingdom") can give cyber criminals the foothold they need to orchestrate such an attack. Key executives' emails and passwords can be sold and purchased on onion sites in the dark web, which can lead to account compromise and exploitation of your company's confidential information.



Threat actors can also publish more coordinated attack campaigns against financial services companies with fraud kits that dupe your customers out of their account credentials.

DOXING 101

Definition: an internet-based practice of gathering identifiable information about a person with the objective to shame, scare, or blackmail the target.

In the U.S., doxing is a form of stalking and is illegal under many different federal and state laws, depending on the exact facts and location.

DOX

Full name: [redacted]
Phone number: [redacted]
Email: [redacted]
Company name: [redacted]

Address: [redacted]
City: [redacted] State: [redacted]

Facebook: [redacted]
Twitter: [redacted]

Credit card: [redacted]
SSN: [redacted]

Reputation risks

We live in a digital age where people will sometimes vent online about a company or flame its executives. This can be a one-time cyberjab but, often, threat actors turn up as antagonists who use profanity and hate speech to create a stir about a key executive and disrupt their day-to-day lives.

THREATS TO YOUR KEY LOCATIONS

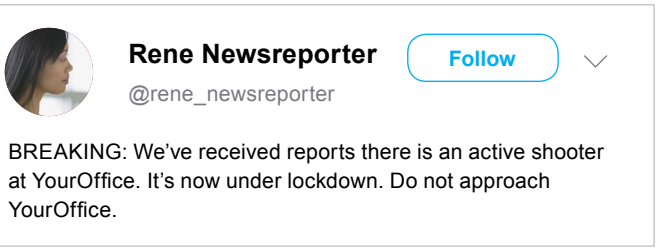
Political tension and conflict escalation in several regions combined with the global economy have created more security risks for protecting a company's physical assets. Physical locations can include everything from a company's secret data center, critical infrastructure assets, retail locations, and corporate headquarters. Whether these are planned attacks against your company or active events occurring near your physical assets, you need situational awareness of real-time risks to your organization.

Threatening language

Organizations should monitor the digital universe for threatening language from suspicious and disgruntled individuals who are in and around your key locations. These can lead to critical events around populated areas, such as concerts, corporate-hosted events, holiday parades, sports arenas, and more.

Lone wolf attacks

For the safety of your employees and customers, your organization needs to be aware of real-time threats and events in and around your key locations, such as your corporate headquarters and retail sites. This can include malls, parking lots, business parks, and frequently accessed locations, such as airports.



According to U.S. Department of Homeland Security, "In many cases, there is no pattern or method to the selection of victims by an active shooter, and these situations are by their very nature unpredictable and evolve quickly." While these threats are out of your company's control, you can manage the risks when your company is made aware and has a plan to mitigate.

Protest

Corporate boycotts and protest events aim to undermine a company and tarnish its brand. Even larger protest movements against economic and social inequality can impact your employee safety and disrupt operations. Coordinated events and actions that occur at business locations and critical infrastructure prevent successful day-to-day business and can be especially harmful to vital infrastructure, such as hospitals, emergency response systems, and energy systems that have physical assets and projects in areas where people are protesting or rioting.

PROOFPOINT EXECUTIVE AND LOCATION THREAT MONITORING

Proofpoint Executive and Location Threat Monitoring helps you gain situational awareness of potential threats against your executives and locations. Our solution crawls the far reaches of the digital world spanning millions of web pages and social sites daily to help you get in front of threats, whether they are planned, imminent, or occurring in real-time.

Executive and Location Threat Monitoring helps you:

- Detect threats on social media and all areas of the web
- Protect your executives and locations
- Gain detailed, real-time threat monitoring
- Increase cyber intelligence and peace of mind

LEARN MORE

To learn more visit www.proofpoint.com/executive-and-location-protection