THE ENTANGLED ENTERPRISE: CYBERSECURITY IS PERSONAL

Targeted attacks against the personal digital lives of high value targets are often more disruptive, and result in larger payouts for hackers, than direct attacks against the enterprise.
The costs of global cybercrime are projected to reach $6T annually by 2021.¹ It is no wonder that today’s executives view cybersecurity as the risk of greatest concern for their businesses.²

Against this backdrop, enterprises have elevated cyber operations and are spending billions on cybersecurity capabilities and infrastructure.

**An escalating cyber arms race**

As global information security and privacy threats are continuously evolving, corporate security teams, human resources departments, legal offices and committees of boards of directors are racing to stay ahead of attackers. Across sectors and industries, organizations are focusing primarily on two categories of cyber risk:

1. Attacks against the *traditional enterprise* (corporate devices, networks and information);

2. Attacks against the *extended enterprise* (third parties – such as outsourced IT, cloud providers, managed services, contractors, other vendors, and even customers).

This is not surprising. As a result of a growing global network of organized cyber criminals, and the commoditization of exploits, organizations must manage a persistent onslaught of threats against legacy infrastructure.

In addition, technology and human capital trends have pushed enterprises to prioritize new threats that are emerging through a simultaneously expanding and fading enterprise perimeter (whether due to the demands of the mobile workforce, the explosion of the internet of things or the increasing reliance on cloud services).

The numbers speak for themselves. The rates of indiscriminate attacks against the enterprise and third parties are daunting. Whether the billions of ransomware attacks (with ransomware variants increasing 50% this past year), the almost doubling of new mobile malware variants (with tens of thousands of malicious mobile apps blocked each day), or the staggering 600% increase in attacks against IoT devices this past year,³ it is understandable why organizations focus on these two categories of risk.

---

¹ Cisco/Cybersecurity Ventures 2019
² World Economic Forum Executive Opinion Survey, 2017
³ Symantec 2018 Internet Security Threat Report, Vol. 23
Yet, a third category of enterprise cyber risk, *entangled enterprise risk*, is conspicuously absent from the budgets and board rooms of most companies.

Entangled enterprise risk includes attacks that cause massive harm to organizational assets and operations but have received little attention and almost no resources.

Who in your organization has responsibility for this category of risk?

Targeted attacks on the entangled enterprise

Entangled enterprise risk is the risk borne by an enterprise from targeted attacks against the personal digital lives of the enterprise’s executives and other high value targets (HVTs). These HVTs often include senior executives, board members, executive assistants, and their family members. Such attacks target aspects of personal cybersecurity that are entangled with the assets of operations of the corporate enterprise.

The security community knows very little about targeted cyber attacks. In its annual Internet Security Threat Report, Symantec acknowledges that targeted attacks – directed at a specific target or targets as opposed to widescale indiscriminate campaigns – are difficult
to measure simply because they are low in numbers.\textsuperscript{4}

Targeted attacks, however, do share a number of common characteristics. They are usually singularly motivated (whether by theft, disruption, sabotage, or intelligence gathering); and, while operationally sophisticated, they often utilize commodity exploits (as exemplified by the December 2018 doxing of German politicians or the rising targeted ransomware attacks).\textsuperscript{5}

Despite being small in number as compared to indiscriminate attacks, the risk posed by targeted attacks is very high. Importantly, while target attacks are frequently directed at the enterprise and extended enterprise, this risk is even higher when it comes to the entangled enterprise.

This entangled enterprise risk includes two categories of targeted attacks against the personal digital lives of HVTs: (1) pivot attacks, and (2) endgame attacks.

**Pivot attacks** leverage vulnerabilities in the personal digital lives of HVTs (including those associated with credential reuse, impersonation, BYOD and mobile work) as a launching pad to gain access to enterprise, and extended enterprise, systems and resources. They take advantage of the fact that senior leaders have access to a wide range of sensitive corporate information, are constantly on the move, and inevitably have personal devices which connect to corporate networks.

Pivot attacks often also leverage compromised personal devices and accounts for reconnaissance and intelligence gathering related to corporate assets and operations. They then take advantage of information collected through compromise of executives’ personal digital lives (e.g., travel plans, family health issues, personal finances) to launch social engineering or business email compromise attacks against employees and gain direct access to enterprise systems or resources.

---

\textsuperscript{4} Symantec 2018 Internet Security Threat Report, Vol. 23

\textsuperscript{5} SophosLabs 2019 Threat Report
business documents from an unprotected home printer). They also take advantage of the fact that compromising senior leaders’ activities, private communications, family life, finances and physical locations can have detrimental effects on business operations (e.g., causing loss of productivity, stealing business critical information, ruining reputations, or extorting business leaders).

Importantly, endgame attacks harm the enterprise without hacking the enterprise.

They are executed entirely outside the enterprise, or even extended enterprise, security perimeter.

Impact

Incidents related to the personal digital lives of executives are not only inconvenient or embarrassing to their companies, they can be catastrophic. Three primary factors have elevated the harm that can be attributed to personal compromise associated with entanglement risk.

1. Faded Boundaries

The interconnections across networks, devices and accounts have created a new reality where the crown jewels of organizations and individuals are no longer locked in a solitary, highly guarded tower. Rarely is there a situation where sensitive corporate information can be exclusively contained in restricted enterprise systems.

Even in the highly hardened national security sector, where compartmented information and systems are standard, high ranking officials are still caught using personal devices and accounts for official business.

2. Digital Dependence

The disruption to business operations and productivity that is associated with the unplanned down time or sabotage of executives’ personal IT is extreme. In today’s hyper connected world, hackers can immobilize, stress, and even cause physical harm to executives via their personal digital lives. The possibilities are limited only by a hacker’s imagination, whether:

- Disclosing details about a CEO’s deteriorating health stolen from a compromised home-connected medical device as a means to influence a company’s stock prices;
- Holding an executive hostage by breaking their connected gate system so they miss an important flight; or
- Tracking the physical location of family members through malicious apps on their devices in order to
harass and extort an executive in the midst of a high stakes business deal.

3. Online Reputation

Lastly, the proliferation of social media services has created an environment where a company’s brand is more susceptible to swings in public opinion than ever.

When, on average, more than 25 percent of a company’s market value is directly attributable to its reputation, the entanglement of a company’s reputation with that of its individual leaders can result in high dividends for hackers. According to one recent study, hackers are making $360k per year for personal cyber extortion. Likewise, defacing the personal social media account of a high-profile executive can be a bigger win for a hacktivist than defacing the company’s official page.

---

6 World Economic Forum, 2012

7 Photon Research, “A Tale of Epic Extortions,” 2019
So, What Does Entanglement Risk Look Like?

As a subset of targeted attacks, entanglement risk is not well tracked or monitored, and compromise can go on for months or years undetected. However, the following is a list of Pivot and Endgame attacks observed in the real world, which should give enterprise security teams pause.

<table>
<thead>
<tr>
<th>THREAT</th>
<th>ENTANGLEMENT</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate documents printed at home + Commodity compromise of home printer</td>
<td>Theft of sensitive financial report printed at home in advance of earnings call used for stock price manipulation</td>
<td></td>
</tr>
<tr>
<td>Enterprise systems accessed from home office + Hijacked home router</td>
<td>Man-in-the-middle attack resulting in executive disclosing login credentials for enterprise systems</td>
<td></td>
</tr>
<tr>
<td>Sensitive corporate technology brought in preparation for business travel + Insecure, internet connected home security system</td>
<td>Physical security system remotely disabled to allow unimpeded access to executive’s home and local access to or theft of corporate technology</td>
<td></td>
</tr>
<tr>
<td>Password reuse between corporate and personal accounts</td>
<td>Privileged access to business accounts with third party vendor used to reroute shipments and steal valuable property</td>
<td></td>
</tr>
<tr>
<td>Personal social media and celebrity used to promote the organization + Unmonitored social media footprint</td>
<td>Fake social media accounts impersonating corporate influencers used to diminish brand image</td>
<td></td>
</tr>
<tr>
<td>Spouse’s insecure personal cloud-hosted photo storage</td>
<td>Threat of leaked images used to blackmail the executive and influence corporate decisions</td>
<td></td>
</tr>
<tr>
<td>Malicious apps installed on a child’s phone</td>
<td>Geotracking used to physically harass and intimidate to influence executive’s position in a company labor dispute</td>
<td></td>
</tr>
<tr>
<td>Ransomware infection on a personal laptop + BYOD</td>
<td>Ransomware infection of corporate network</td>
<td></td>
</tr>
<tr>
<td>Hacked personal email</td>
<td>Malicious spear phishing emails sent to coworkers result in compromise of company networks</td>
<td></td>
</tr>
<tr>
<td>Use of insecurely configured personal phone on insecure public WiFi</td>
<td>Personal information of business contacts stolen and used for spamming and doxing, harming key business relationships</td>
<td></td>
</tr>
</tbody>
</table>

This list, however, is only scratching the surface. Because entanglement is largely a function of the unique and constantly shifting personal digital life of a given executive, the scope of entanglement risk for any enterprise is only limited by a hacker’s imagination.
About

Cypient Black provides holistic coverage for the personal digital lives of executives and their families. The Cypient Black cyber executive protection platform delivers enterprise-grade personal cybersecurity protections that are an essential complement to organizations’ corporate risk management and cybersecurity capabilities. Through the use of automation, advanced analytics, and a deep understanding of user behavior, we are reshaping the digital landscape.

Contact Us

www.cypientblack.com
800-208-1455

Copyright © 2019 Cypient Black. All rights reserved.