TAG CYBER

DELIVERING DIGITAL EXECUTIVE PROTECTION: AN INTRODUCTION TO BLACKCLOAK

DR. EDWARD AMOROSO, TAG CYBER

BLACKCLOAK

TAG CYBER

DELIVERING DIGITAL EXECUTIVE PROTECTION: AN INTRODUCTION TO BLACKCLOAK

DR. EDWARD AMOROSO

The need to provide concierge digital security support for corporate executives, high-access employees and prominent individuals has become well-established. Security start-up BlackCloak addresses this need through its Digital Executive Protection (DEP) solution that minimizes cybersecurity and privacy threats to these targeted individuals and groups.

INTRODUCTION

Enterprise teams have come to the recent understanding that an executive's personal digital presence has a significant impact on organizational cyber risk. When key personnel exercise sloppy security in their personal use of online accounts and services, or fail to remove personal data from online data brokers, exploitable risks emerge that can be targeted by bad actors. Risks also emerge from vulnerable home networks, unprotected personal devices and online accounts—not just of the executive, but also their families.

This report introduces and explains a new discipline known as *Digital Executive Protection (DEP),* which is increasingly becoming a mandatory aspect of enterprise protection initiatives for corporate executives, board members and senior leaders with access. This approach also can be used to protect prominent, well-known individuals who must exercise prudence in their online presence to avoid targeted threats.

The commercial solution from BlackCloak provides effective DEP support for corporate enterprise buyers when it comes to protecting executives and other prominent individuals who are concerned with emerging digital risks to their business, personal finances, reputation or safety.

THE RISKS OF PERSONAL DIGITAL INFORMATION, DEVICES AND ONLINE PRESENCE

Digital risks to executives and prominent individuals span both cybersecurity and privacy. They emerge based on the so-called *personal digital lives* of these individuals, resulting in a concept often referred to as an attack surface. The most common risk elements associated with an executive's attack surface include the following threats, each of which are currently occurring on a regular basis:

- *Targeted Attacks*. Executives and their families are commonly targeted for the purpose of financial attacks and online fraud, which can result in personal losses for the individual and their family, as well as be used to go after the assets of an enterprise. Online fraud is made easier by the mass availability of personal information— including cell-phone numbers, personal emails, home addresses, home IP addresses and other information—via online data brokers and social media.

- *Identity Compromise*. There is a high potential for executives and other prominent individuals to lose their privacy and have their personal information stolen, which can then be used to open accounts, create tax fraud or purchase items. It can also be used to target enterprise resources if a company relies on personal information for authentication and authorization tasks, making identity theft a serious concern. Identity compromise can also lead to corporate data compromise and increase the likelihood for reputational attacks against an executive and the company.

- *Modern Digital Threats*. In addition to fraud and identity compromise, executives must contend with additional risks originating in the home or on personal devices. These include: reputational attacks through deep fakes; phishing attacks to plant malware on personal devices and networks; and social engineering attacks aimed at a variety of different objectives. Prominent individuals and, by extension, their organizations must be on guard to avoid these risks, but they can also benefit from professional security assistance.

Organizations must pay close attention to these personal risks, because malicious actors now recognize that the path of least resistance to an enterprise's data, assets and resources exists through targeted executives. In other words, adversaries have learned that an executive's personal digital attack surface is a much softer means for gaining access to an enterprise, as opposed to trying to get through the layers of in-depth defense controls that protect a company's key assets.

An additional complication is that enterprise audits, assessments and reviews rarely consider the digital behavior and personas of their executives. The culture of enterprise security has maintained a focus on business assets, while the privacy of executives and their families has been considered a higher priority than the investigation of potential risk. This decision must be reconsidered, as the risk to executives continues to grow.

WHAT IS DIGITAL EXECUTIVE PROTECTION (DEP)?

A new form of cybersecurity protection has emerged known as *digital executive protection (DEP)*. The purpose of DEP is three-fold: namely, to reduce the personal digital risk of a targeted individual; diminish the risks associated with an individual's family and inner circle; and finally, lessen the risks associated with a targeted individual's enterprise or organization.

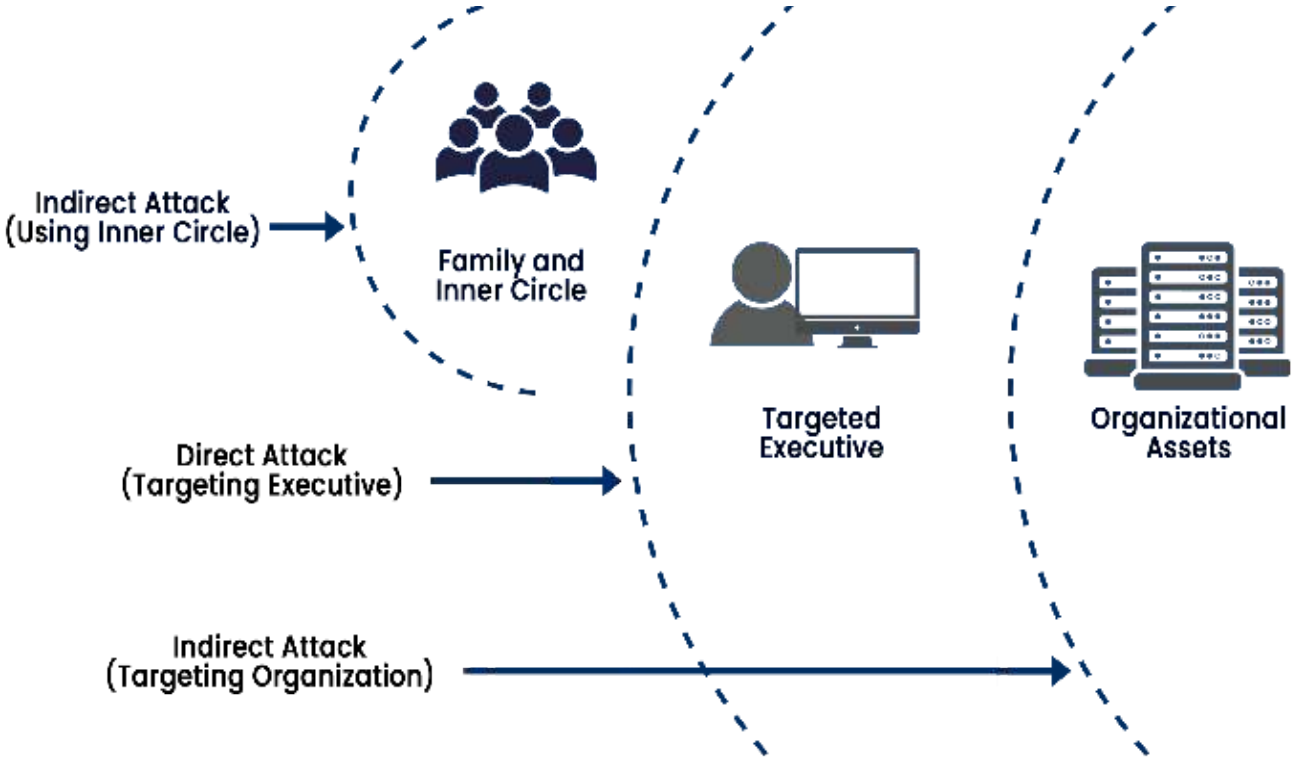

Figure 1. Indirect and Direct Targeted Attack Cases

The manner in which DEP is offered varies between different commercial providers, but, in most cases, it includes a combination of technology, expert availability and supporting resources. This unique mix for executive protection requires that a DEP solution provider fully respects the many different requirements of its customers. Specifically, the following must be taken into consideration in any successful offer:

- *Privacy of Targeted Individuals*. Executives use personal online accounts for private, nonbusiness-related functions. These include community, family, church and other private activities, as well as sensitive communications with doctors, counselors or even competing enterprises. To this end, the DEP solution provider must ensure full privacy in all supporting activities.
- *Privacy of Executive Families*. Since most executives integrate their personal digital persona with that of their family through shared Wi-Fi, e-commerce accounts, streaming services, etc., it becomes important for DEP providers to recognize and protect the privacy of all involved. Family members often include minor children who require extra care when it comes to protecting their privacy.
- *Separation of Individual and Organization*. While executives recognize that protecting their personal information brings value to the organization, they may also be hesitant when it comes to exposing their private communications and accounts with the company. To that end, DEP providers must ensure there is a separation of attention between the executive and the company, much like the separation that exists with healthcare benefits.

In the next section, we introduce a new commercial solution that includes many aspects of required DEP functionality, while also paying attention to the basic privacy and separation considerations listed above. The offering from cybersecurity vendor BlackCloak combines technology, experts and resources in an arrangement that is well-suited to the needs of the modern executive.

OVERVIEW OF THE BLACKCLOAK PLATFORM

Founded in 2018 by Dr. Chris Pierson, BlackCloak provides concierge digital executive protection (DEP) services for executives, C-suite members, board directors, high-access employees and other prominent individuals. The objective of BlackCloak's DEP offering is to address the personal cybersecurity and privacy risks of these individuals, along with the additional goal of reducing transitive risks to their organizations.

The commercial BlackCloak Concierge Cybersecurity & Privacy Platform includes the following DEP capabilities for customers, families and their associated enterprise organizations:

- *Platform Features*. The BlackCloak platform offers a desktop and mobile experience for customers that addresses risks to endpoints, online accounts, personal networks and other relevant assets of interest to an executive and their inner circle. This platform also provides protection for their personal privacy by removing data-broker data and exposing any dark web risks.

Figure 2. BlackCloak Desktop and Mobile Application

- *Concierge Support*. BlackCloak experts are available on demand to provide real-time security recommendations for customers. Strategic actions are tailored to the executive's personal situation, and a US-based security operation center (SOC) is available to offer guidance, support and full incident response to the executive, their family and the organization. This support covers all aspects of personal privacy and cybersecurity.

BlackCloak also includes an educational portal that helps customers make better decisions about their personal digital lives. The goal is to ensure that the executive is placed in a more secure personal ecosystem that combines technology platforms, expert support and guidance, and the ability to self-learn the most important basics of digital protection. Organizations obviously benefit when their executives enjoy this feature.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: Dr. Edward G. Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.