BLACKCLOAK™

Executive Protection: What Will You Say When Asked?

BlackCloak CEO Chris Pierson on How to Discuss Cybersecurity in Personal Lives

ISMG INFORMATION SECURITY MEDIA GROUP

BLACKCLOAK™

So what happens when you as a security leader get that call to protect the cybersecurity of executive leaders and board members outside the office? What are the right and wrong responses? **Chris Pierson** of **BlackCloak** shares new insight on executive protection best practices.

In this video interview with Information Security Media Group, Pierson, the founder and CEO of BlackCloak, discusses:

- The right and wrong responses to queries;
- Why it's a problem if you aren't even being asked;
- Who needs to initiate and advance this discussion.

The Wrong Response

TOM FIELD: When security leaders get that call to protect executive leaders and board members outside the office, what is the wrong response, based on examples you've seen?

CHRIS PIERSON: In many cases, one of the biggest problems is that executives are not getting that call. They're having to start that conversation themselves. They've worked so hard to protect things on the inside of the four walls of the company, but there's this big gaping hole out there.

There are two wrong responses. One is: "Don't worry; my team and I will take care of it." That means you're using corporate resources in the personal lives of the executives, the spouse, significant other, kids, all the rest. You've completely blurred the lines of personal and work. What policies apply? What reporting requirements do you have? What happens if you spot something that's an ethical issue or an HR issue? You now have people that

Dr. Chris Pierson

Pierson is the founder and CEO of BlackCloak - a concierge cybersecurity protection suite for high-net-worth individuals and top C-Suite executives. BlackCloak protects its customers from financial loss, cybercrime, hacking, reputational damage, privacy exposure and identity theft. In addition to his role at BlackCloak, Pierson serves on the Department of Homeland Security's Data Privacy and Integrity Advisory Committee and the DHS Cybersecurity Subcommittee. He has been on the front lines of cybersecurity and fighting cybercrime for over 20 years - with DHS, as president of the Federal Bureau of Investigation's Arizona Infragard and as a chief information security officer for financial companies. He was a founding executive of Viewpost, a FinTech payments company, and served as its CISO and general counsel. He was the first chief privacy officer, SVP for the Royal Bank of Scotland's U.S. operations and was a corporate attorney at Lewis Roca Rothgerber Christie, for which he established a cybersecurity practice.

> "One of the biggest problems is that executives are not getting that call. They're having to start that conversation themselves. They've worked so hard to protect things on the inside of the four walls of the company, but there's this big gaping hole."

are being paid by the company involved in the personal lives of people that are at the upper echelon of the company – board members, directors, C-suite folks. That's a bad way to do things.

The second wrong responses is – and no one does this anymore – offering an antivirus DVD or consumer-grade antivirus or some free credit monitoring. The unique risks of this unique population are not going to be solved through a consumer-based solution or by having a white-glove concierge do 24/7/365 monitoring and protection.

The Right Response

FIELD: What's the right response?

PIERSON: First of all, something that's holistic. These people lead unique lives that are inextricably tied and intertwined with the company. Elon Musk is Elon Musk, but he is also the CEO of Tesla and SpaceX. He ties back into those organizations. So make sure that you have a holistic response that solves both privacy and cybersecurity.

What does that mean? Let me give you an example. A corporate executive had their profile online, at data broker websites, but usual removals weren't good enough. Some of the profiles they wanted information removed from were very specific for their industry. BlackCloak was able to do that. Holistic protection includes privacy, data broker removals and dark web removals, device protection, home protection and a concierge. The threats to the corporate executive are happening in live real time, 24/7/365. And it's not just the executive you have to protect. It's the family group too.

CISOs: Take the Lead

FIELD: What if security leaders aren't getting these requests, and they wish they were? We've heard that over and over this year.

PIERSON: Executives are the most targeted group, and the CISO is the person who has to broach this. It's incumbent upon us as security professionals and privacy professionals to start that conversation and move it up into the board room and the C-suite. The executives that we talk to are all worried about this. They ask: "Why are my home addresses online? What can you do about it? How do I make sure that while I'm working, the kids and my spouse or

significant other are not clicking on things causing vulnerabilities at home, because I often work from home?" They were asking these questions pre-COVID-19 and now it's much worse.

FIELD: Who needs to start this conversation about protecting digital lives outside the traditional office?

PIERSON: The CISO. If you're a chief information security officer, you know that these risks abound for executives in their personal lives. Start the conversation now. Second: Get partners. For example, the chief financial officer wants this solved so an incident doesn't occur that costs the corporation a lot of money. They want to protect the money, the reputation and the branding of the company. And when you talk about reputation, the CFO also wants this solved. The head of HR and executive benefits wants this solved and so does the general counsel. So call in your partners, grab your other C-suite fellows and friends and start that conversation.

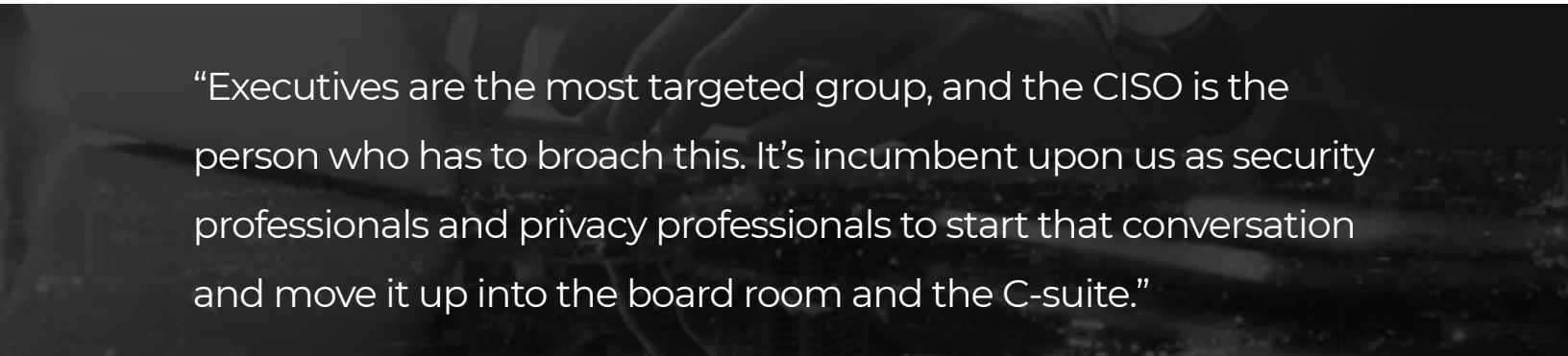
FIELD: Is this a shared responsibility? Who needs to own this?

PIERSON: Whatever happens – unemployment fraud scams that hit corporate executives, filing for small business loans to hit corporate executives, data breaches in the personal lives of the executives, the car dealership, the trading platform, their personal email – whatever it is, the incoming is going to be ones and zeros. They're going to turn to you, the CISO, and to the CTO and the CIO. You're almost always going to be involved. So you might as well start the conversation.

A Third-Party Role

FIELD: Who does the job? Is it in-house, outsourced or hybrid?

PIERSON: You do not want internal persons in the personal lives of the executives, their significant others and their families or in the personal lives of the board members – for a whole bunch of privacy and legal reasons. It's definitely a third party task. This model is used in healthcare. For example, everyone at Acme Corp. has Cigna healthcare. For the executive team, they have a concierge doctor on call 24/7 and concierge physicals through a third-party medical provider. The company pays for the executives' benefits, and their personal lives and are protected. And if something bad happens, the right response team is there.



"Executives are the most targeted group, and the CISO is the person who has to broach this. It's incumbent upon us as security professionals and privacy professionals to start that conversation and move it up into the board room and the C-suite."

OUR STORY

We founded BlackCloak to unite the top leaders in cybersecurity, privacy, and engineering to solve this growing challenge. Informed by decades of experience, our team has developed a concierge privacy and cybersecurity platform that measurably protects every aspect of your digital life. Merging enterprise-grade technology with expert advice, guidance, and education, we deliver concierge-style plans that match the unique threats our clients face. With BlackCloak, you can protect your digital life — and your peace of mind — anytime, anywhere.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® (Just for Credit Unions) GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY (Prevention. Response. Notification.) CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io