Cyber Whaling – Part IV

What Are The Three Levels of Executive VIP Cybersecurity And How Is Your Organization Leaving You Financially & Reputationally Exposed Across Them?

In the last three research notes, we discussed (1) why leaders must think differently of their cybersecurity vs. that of their organization, (2) the cyber-whaling statistics and environment that are causing havoc for affected private and government sector leaders as targets for hackers, and we provided you with (3) a case study that should make any leader think twice about ignoring the risks of cyber-whaling. Now that you've understood the outsized risk you face, financially and reputationally, you also need to understand the three levels of Executive VIP Cybersecurity and the differences among them:

Figure 1: The 3 Levels of VIP Cybersecurity & Their Risks

a. **Level I:** Your cybersecurity as the leader of your organization; vs.
b. **Level II:** Your cybersecurity as a private citizen; vs.
c. **Level III:** Your family's cybersecurity.

Each of these three Levels' cyber(in)security has a direct and indirect effect on the other two, and risk of one spreads 'free-flowingly' to the other two. Therefore, you must not only pay attention to the risks emanating from each level but understand how the risks of each level differ from the other two. Not understanding these three levels' differences, as well as the tactics necessary to prevent the serious consequences caused by ignoring their differences and filling in the risk gaps with the necessary tools can be the reason why you get breached and your organization is forced to part ways with you or to shut down altogether (note: 60% of small organizations shut down within 6 months of a breach and there is no better way to shut an organization down than to attack it through the executive).

To better understand the differences among these three levels, let's consider what your organization does and doesn't generally provide you with in terms of cybersecurity and cyber insurance across each of these three levels. This way, you can gain a sense of the gaps you need to fill in and the tools that such an exercise might require.

LEVEL I

In terms of your professional cybersecurity as the organization's leader – the executive VIP – your organization rarely if at all covers you at the level of the threat landscape facing specifically you as the VIP, either because of insufficient cybersecurity expertise, budget, or policies, all three of which are common and are in turn driven by:

1. Insufficient Awareness of the VIP-specific Threat Landscape – which hackers are targeting you, why, etc.;
2. Insufficient Awareness of the VIP-specific Threat Vectors, i.e. what methodologies do hackers use against you that you need to be aware of;
3. Insufficient financial resources for 24/7 VIP-Level Threat Management, because if your organization tried to manage its cybersecurity at the level of threat landscape facing you, it would erode most of your organization's profit margins quite quickly;
4. And finally, insufficient Understanding of & Planning for the Interaction of Professional, Personal & Family Risk, and how each risk affects the organization.

These reasons are enough for an organization to almost never sufficiently protect your cybersecurity as a professional, i.e. the organizational VIP.

LEVELS II & III

And to add to this, your organization generally never covers your personal cybersecurity, or that of your family. But you actually don't want it to, either, because you don't want your CTO, CIO, CISO or your Board to know what you're doing on a weekend that may not be entirely condoned by the organization, something they'd know if they covered your personal & family cybersecurity. Let's say you're looking for another job… You probably don't want your organization to know that. Or do you want them to see your texts between you and your wife? Probably not. Would you want them to know what your teenage kid is doing online? Probably not… And so when it comes to protecting you at the personal and family level, you're entirely on your own, and rightfully so.

And yet, when a cyber breach at any one of these three levels – professional, personal, or family – inevitably occurs and your organization is negatively affected (reputationally, financially, or otherwise), your organization will likely need a scapegoat – very likely you – further putting your own reputation, finances & your family at risk.

CYBER INSURANCE:
And unfortunately, as of the present moment, most organizations do not provide you with any cyber insurance either, for you as the leader of your organization and certainly not for you as a private citizen, or your family.

So you are fully exposed, especially at a time when you might be working from your less cybersecure private home networks during the COVID-19 pandemic.

And even if you do have professional, personal, or family cyber insurance, most cyber insurance policies out there still aren't worth the paper they're printed on because the cybersecurity threat landscape is changing so rapidly and policies simply can't catch up, and so you have to behave in a cybersecurity-first way as a preventative measure rather than using cyber-insurance as an after-the-fact band-aid. Furthermore, cyber insurance policies are too often legalistically written in a way that protects the insurer downside, not yours (see our previous research note Case Study that demonstrates how a CEO & CFO were taken by a $1.85mm cyber-insurance "surprise").

KEY TAKEAWAYS:
And so (1) you're not fully protected professionally, and (2) you will never have your organization cybersecure your personal or family life since that would mean a serious violation of your privacy, (3) cyber insurance is limited at best, and so that leaves you with no choice but to take control of and own your professional, personal, and family cybersecurity yourself and do so with a level of seriousness and vigor.

To Access Previous Cyber Whaling Report Posts:
1) Part III – 2020.11.25: CASE STUDY: For Corporate Executives, Entrepreneurs, Boards, Investors
2) Part II – 2020.11.24: Why Should You (Really) Care About Cyber Whaling If You're A Business Executive, Board Member, Political Figure, Entrepreneur, or Government Official, aka "Organizational VIP?"
3) Part I – 2020.11.23: Why must business executives, Board Directors, politicians, entrepreneurs & other leaders focus on their cybersecurity differently than cybersecurity of their broader organization?
4) Intro – 2020.11.20: Why are Organizational VIPs such a perfect target for hackers and why am I therefore obsessed with helping leaders avoid these attacks?

About the Author: Andrzej Cetnarski is a national & cyber security strategist, Founder & CEO of cyber defense ecosystem Cyber Nation Central® & Executive Producer of VIP Cybersecurity Blueprint™, an "A-Z Manual for VIPs' Professional, Private, & Family Cybersecurity." Formerly an investment banker with UBS tech & real estate groups & Chairman/CEO of a global tech & hospitality venture, he is an alumnus of Harvard's Kennedy School of Government, The Wharton School, & the University of Chicago, & writes on integration of strategy, tech innovation, and policy in the areas of cybersecurity, national security, countering disinformation campaigns, and privacy.