Who are the Cyber Criminals?

By Assurance Software on Jan 9, 2019

Cyber crime. We know it can victimize and disrupt all businesses, in every industry, anywhere in the world. But who's actually doing the hacking? Do you envision a lone villain, cloaked in a dark hoodie and malicious intent, drumming his fingers over a dimly lit keyboard in a damp basement? Or is it the ponytail-wearing, triple-espresso gal slumped in front of her laptop next to you at the coffee shop? Let's find out...

This past year, Nuix, a software tech company, conducted a unique survey: The Black Report. They wanted to go where no other cyber survey has gone before: inside the minds of hackers. Their goal was to understand the minds of cyber criminals and gain a better understanding of their methods, attitudes, and overall, who they are. Enterprise insiders, lone thrill-seekers, collaborative factions, college graduates, high school dropouts, unemployed persons, career-professionals...or all the above?

Understanding who the hackers are and how they operate boosts organizations' ability to combat cyber breaches, mitigate loss and damage, and therein fortify their business continuity. So, let's take a look behind the cyber door and see who's there...

Behind the Cyber Door

For the report, Nuix defined a hacker as: a person who accesses computer applications or systems without permission in order to perpetrate malicious activities for personal gain.

15% admit to accessing an employer's data for personal gain

First up, the results purged the out-of-work, basement-dwelling dark actor perception. A substantial **39%** of respondents work for large businesses; **36%** are employed by small and medium companies; **16%** are with small consulting agencies; only **9%** reported being "self-employed."

ARE THEY EDUCATED?

And as would be expected with the number of big-business employees, many are educated as well: **43 %** are college grads and **32%** hold postgraduate degrees. Only **19%** stopped their education after graduating high school, with **6%** opting out even sooner.

Additionally, **60%** acquired up to three professional certifications, with **22%** holding three to five; **13%** have between six and ten, and **5%** boast more than ten. Further insight was garnered by **78%** of all admitting that they felt certifications were not necessarily a qualifier for technical abilities. Rather, they see technical certifications as means "to secure employment, remain relevant, and advance their careers."

61% believe they knowingly broke cyber security laws

HOW LONG HAVE THEY BEEN HACKING?

Time served seems to be almost evenly distributed: Only **10%** have been at it less than three years; **19%** have been hacking between four and six years; **16%** have been in the arena for seven to ten years; and veterans with more than 17 years wraps up **15%**.

DO THEY HACK THEIR OWN "HOUSE"?

Not surprisingly, some hackers access their employer's sensitive data without authorization: **14%** admitted to invading critically valued data (CVD) for purposes outside of their job requirements. That may seem like a small number, but consider this perspective: for **every 1,000 employees**, **140** may be wrongfully dipping into your data. Worse yet, **35%** revealed they have taken enterprise data when they left an employer.

These numbers make the case for stringent internal security protocols as well as external ramparts. The unknown outsider is not your only threat.

86% claimed they hack for the challenge

WHY DO THEY HACK?

And finally the most insightful question of all: Why do they do it? Think it's for money? Not always: Only **21%** cited financial gain as a motivation; **86%** claimed they hack for the challenge and to learn; **6%** are in it with political incentives; and **35%** hack for kicks. (In the survey, respondents were permitted to select multiple answers.)

Those results are reinforced by **44%** admitting they must use "a lot of self-control to stay out of trouble," **54%** indicating that "life with no danger would be too dull for me," and **68%** enjoy taking risks. It's the thrill of the hunt.

Additional research and literature support these findings and suggest if a person has close ties with other hacks, is not involved in frequent or conventional social activities, has little to lose if caught, and does not harbor moral qualms about following rules and laws, there's little to bar one from hacking at will. If this is compounded with additive motivations such as revenge or financial necessity, it's all the more enticing.

WHO DO THEY HACK?

Ultimately, hackers are opportunists. They seek the easiest target, like a lion going after the wounded gazelle. And several industries offer them easier prey. These sectors bear a general tendency towards sub-par cyber security:

- Food and beverage
- Hospitality
- Retail
- Hospitals and healthcare providers
- Manufactures
- Sports and entertainment companies

ADDITIONAL FACT BYTES

- Most hackers can penetrate a target system within 15 hours
- 88% employ social engineering to gain knowledge of their target
- 80% take advantage of free tools easily obtainable on the internet
- 70% use forensic tools or other methods to cover their tracks
- 93% believe their targets only detect 50% of the attacks
- Average gap between a breach and its detection is 200-300 days
- Ransomware attacks increased 300% between 2016 and 2017, with a daily incident rate of 4,000
- 9 out of 10 organizations fail to address all the vulnerabilities they discover during penetration tests
- 100% hackers agree your data is gone once your perimeter is breached

What Does It All Mean?

What can organizations glean from this study to augment their cyber security efforts? In one sentence: Assume a cyber attack is imminent. Always. The primary motivation driving hackers is "because I can." Though some harbor additional goals, this reason is largely of an un-reproducible nature. Even the preference for easier targets doesn't hold as much weight when they're simply in it for the challenge. The thrill may be sweeter the more difficult the breach.

Add to this that hacking is no longer a long-acquired skill of the tech-savvy. Really, anyone with intent can lay a cyber siege upon a desired target. The dark is awash in cyber crime "how-to" schemes and downloadable hacking code (cyber-crime-as-a-service). And as more and more devices and appliances become connected to the internet opportunities proliferate. In 2017, humans produced 122 exabytes of internet protocol traffic.

"Anyone can be (or hire) a cybercriminal."

The size of your company, nor the nature of your business are not reliable denominators when it comes to predicting cyber crime. Cyber crime is simply everywhere. Every day. All organizations must approach cyber security as if they're the next victim on a hacker's list: build formidable cyber walls and protocols, but also institute a cyber security incident response plan as part of a full-spectrum business continuity plan (BCP), which outlines actionable procedures and processes for responding to a cyber security incident.

Here are a few quick tips to help bolster your cyber security for more resilient business continuity:

QUICK TIPS

- Conduct background checks and vet employees
- Monitor network usage and accesses
- Ensure your organization adheres to industry compliance standards
- Perform regular supply chain and third-party cyber security audits
- Stay abreast of current cyber crime and trends and update BCPs accordingly
- Educate employees regarding cyber security best practices and share cyber trend news
- Determine your most valuable data
- Protect against outside *and* internal infiltration
- Use multiple authentication methods
- Restrict sensitive data to a need-to-know basis
- Institute mandatory protocols for bring-your-device (BYOD) policies
- Cultivate a cyber security culture
- Hire a Chief Information Security Officer (CISO)

Understanding hackers awards valuable information to help your organization bolster your cyber security tools and protocols, and more accurately develop an incident response plan when a cyber outsider does get in.

Cyber impacts can be extremely damaging to your business and reputation.

Assurance Software offers a cyber risk assessment that can evaluate existing business continuity plans, assess your cyber-attack vulnerabilities, test your ability to quickly respond, and recommend action steps.

Get your assessment today.