JS|HELD

PERSPECTIVES

Cybercrime vs. Cybersecurity: Learning the Tactics of Criminals to Protect Your Interests

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Gone are the days where technological solutions were "nice to have" options to provide us with better access to resources and improved process efficiencies. Nowadays, technological solutions – and specifically those that require data to operate – are ubiquitous.

But as we use more data-driven technologies in our lives, have we considered the risks that have been, and continue to be, *created over time?*

Data has been traditionally treated as an asset, which for the most part has been correct, and has resulted in positively impacting our interests. Yet, with the now daily revelations of adversary state-sponsored and digital crime ring attacks, and their associated breaches, data is increasingly beginning to feel like a liability. The reasons are manifold and include stricter regulations and statutes, technological "pacing" considerations, privacy concerns, difficulty to manage large and disparate data sets, and of course, the mountains of data making it into the digital wild, whether through theft, breach, or negligence.

In practical terms, what does this mean for the user? It means threat actors – *who are always at the leading edge of creativity* – now have an innovative method at their disposal to exploit victims: collecting, collating, and using "data in the wild" to conduct targeted attacks against persons and organizations. The necessity to carry out sophisticated technical attacks (e.g., "hacks") diminishes, because threat actors can attack the constant weak point: humans.

Moreover, as the requirement for technical competence to carry out attacks diminishes, the likelihood of non-technical threat actors entering the arena increases. Remember, once upon a time, operating a computer required considerable technical competence. Today though, "computers" (e.g., smartphones) are in everybody's pocket, and even those with limited knowledge can carry out tasks using a sleek graphical user interface.

With this modern context and understanding in mind, this article will outline today's evolving landscape of cyber-enabled fraud, theft, and digital extortion. Moreover, the article will compare the "inside out" approach of cyber***security*** and defensive methods versus the "outside in" method of cyber***crime*** prevention. Finally, we will examine solutions that provide proactive risk reduction measures.

Breach Data, Reconnaissance, and Open-Source Intelligence

There was a time when criminal actors needed to "break in" to acquire data. And of course, many still do today. Breaking in required some type of technical understanding or competence to get around the security measures individuals and organizations put up.

But as with most technologies, evolution happens. For every defensive measure we institute, nefarious actors invent an alternative path. This feedback loop will not change; it is a constant of life. Stopping criminal behavior requires some type of dissuasion or consequence, and for all our efforts, a treasure trove of rogue data has been growing, a pool so large that cyber criminals see it to be so lucrative, they cannot resist using it.

Moreover, it is relatively cheap and convenient for them to access the data too, which means a greater return on their investment. Never forget for *most* cyber criminals, **it is all about the money and the path of least resistance.**

So, what is this pool of data and why does it matter? The pool consists of three main sources:

- **Breach Data.** These data sets are collections of previously stolen or non-public sets now available on the open internet, dark web, or closed hacker forums.
- **Reconnaissance.** Collections of data gathered by accessing or scanning publicly available information on the internet, such as social media and public document disclosures.
- **Open-Source Intelligence (OSINT).** Similar to reconnaissance data, collections of data sets that are gathered from free sources or data brokers.

Individual data points from these data sources can provide detailed glimpses into a person's life, or an organization's business approach. Collectively though, the seemingly benign or unintrusive records of information, ranging in the billions, can be collated, presenting an intimate and detailed picture of the person's life or the organization's advantages and weaknesses.

Building the Dossier for Tailored Attacks

In some cases, these data sets can go back as far as 20 years. When one considers the amount of available data that can be collected and collated, then processed through modern day technologies, computational powers, machine learning, and artificial intelligence, a threat actor can very easily develop a pattern of life or dossier on a potential victim to carry out sophisticated, tailored, and targeted attacks.

Keep this also in mind: the data sets can easily connect you to loved ones and those within your personal and professional circles. Imagine, for example, how a ransomware negotiation can instantly change when a threat actor shows you pictures from your child's social media account.

Furthermore, all this information can then be indexed and searched using simple queries, such as names, dates of birth, or email addresses.

Using the dossier of information, threat actors can perform two primary types of attacks, as we have seen in real cases:

1. Social engineering attacks that can lead to fraud, extortion, or duping the victim into giving more valuable information
2. Unauthorized system access using common or reused credentials, usernames, and passwords

This is what we mean when we say the "outside in" view of the world. Nefarious threat actors no longer need to focus on breaking into a system or network via technical means. Additionally, the reader should now be gaining a greater understanding of how these data sets can be used for both offensive and defensive purposes.

Enhancing Protections to Account for Human Risk Factors

What should be understood is that the "outside in" approach is not a replacement for the "inside out" methodology. Rather, the former bolsters the protections of the latter. So, what do we mean by the "inside out" methodology? Think more of your defensive and traditional approaches, which include:

- **Internal controls**, such as, but not limited to, firewalls, identity access management, multi-factor authentication, data loss prevention, endpoint detection and response, intrusion detection and protection, and threat intelligence platforms.
- **Security programs and assessments**, such as, but not limited to, formalized programs with dedicated staff, assessments, and compliance audits (e.g., NIST CSF, ISO 27000, OWASP, etc.), and external reviews.
- **Training and testing**, such as, but not limited to, phishing simulations, annual compliance tests, network penetration tests, application penetration tests, regular code review, and tabletop exercises, both procedural and technical.

All these efforts are necessary, and well deployed implementation of these defensive measures demonstrates all the hallmarks of a mature cyber*security* program. But as powerful as these controls can be, their effectiveness against cyber**crime**, given the nature of the threat, is diminished. For this reason, an understanding of the "outside in" view of the world, or "human risk" perspective, helps to protect and inform the "inside out" defensive requirements.

Protecting Your Digital Life to Protect Your Interests

Now more than ever, protecting your digital life and your wider interests begins with the individual. For all the technical protective measures in place, individuals need to have "clean digital lives" and proactively protect them as well. The mistake many of us can make is in thinking that the seemingly innocuous data points, while potentially a nuisance or intrusive, cannot come back to harm us. This may be true of single data points, but there are billions upon billions of readily accessible records that can be scanned and used for nefarious intent.

Therefore, the question becomes: do you know what your digital life looks like? Common questions include:

- Was any of my personal information, usernames, or credentials, exposed in past breaches that I do not know about?
- Are those close to me creating additional and unwanted vulnerabilities because of their digital lives?
- Is my information being sold and exposed by data brokers, which can then be further used against me?
- Can my digital life be used against me, my family, or my organization for fraud, theft, extortion, or any other type of similar harm?

The "outside in" review of your digital life effectively gives you a glimpse into what nefarious actors could potentially have at their fingertips to exploit you.

Digital Crime Prevention: How to Thwart Criminals Today and in the Future

Data-driven technologies have made certain aspects of our lives easier and more efficient – *and reasonably argued some aspects more difficult and cumbersome!* Furthermore, these same technologies facilitated the rapid creation of digital lives, ones that we are increasingly dependent on to carry out daily tasks.

A by-product of creating these digital lives though has been the introduction of novel risks; risks that have not been well understood or adequately addressed to date. We have generations, even thousands of years of knowledge to rely on for protecting our physical self; yet we barely have a decade or two of knowledge on how to protect our digital self.

Therefore, the generally accepted "inside out" security-minded approach needs to be bolstered by the "outside in" prevention-minded approach to best safeguard our digital lives and interests.

The old adage of *"knowing is half the battle"* certainly applies in this case: therefore, it is a good time to start knowing more about our digital self before harm strikes.

Acknowledgments

We would like to thank our colleagues George Platsis, Patrick Westerhaus, and Scott Wright for providing insight and expertise that greatly assisted this research.

More About J.S. Held's Contributor

George Platsis is a Senior Director providing Digital Investigations & Discovery services in J.S. Held's Global Investigations practice. Mr. Platsis is a business professional, author, educator, and public speaker, with an entrepreneurial history and upbringing of over 20 years. He has designed and delivered solutions, and led teams, to improve breach readiness, enterprise-wide and business-unit specific incident response programs, and estate hardening for a series of Fortune 100 clients in healthcare, media, financial services, manufacturing, defense, and commercial electronics industries, including support of clients in the small and medium business space. Additionally, he brings complex investigation and emergency management experience to businesses and individuals seeking to reduce their risk posture. He is also a Certified Chief Information Security Officer.

George can be reached at george.platsis@jsheld.com or +1 321 346 6441.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.