themakogroup

Security | Risk | Audit | Advisory

mako

White Paper Series

How NOT to Get Hacked

and other tips and tricks on protecting your organization from a cyber attack

www.makopro.com

A word from our CEO

David Lefever
CEO & Founder

Thank you for your interest in this strategic content, built by professionals with their feet on the ground and their fingers on the pulse of the latest industry trends. The Mako Group is a mid-west based professional services firm focused exclusively on audit, risk, cybersecurity and strategy. Our reputable company is built on a strong set of personal values, and the services we provide are driven by quality. We're here to serve you; to respond to your needs, armor you with knowledge and leave you with a clear conscience.

At The Mako Group, we've built a firm grounded on the principles of risk reduction through the trusted foundations of audit and security. The overall risk profile of your company is as important to us as it is to you, and building peace of mind doesn't come easy. As we build new content, develop new relationships or construct a successful program, we find the formula for success to be somewhat simple. It's all about trust. Most things simply boil down to trust; something you can't buy. Trust is earned. It's earned through honesty, transparency, delivering on your promise, performance through achievement and ultimately through results. Expect the best and accept nothing less.

As a team, we at The Mako Group believe in the power of trust and exemplify this through our actions. With that, we've built a strategic content library of case studies, white papers and infographics just for you. These important perspective pieces are built solely to give you the insight and peace of mind you need to make qualified decisions. They're built to help you sharpen your pencil and shape the instincts necessary to succeed.

We hope you find high value in what you read, and welcome any additional insight or feedback you would be willing to share.

David Lefever
CEO & Founder

themakogroup
Security | Risk | Audit | Advisory

EDITORS
Meredith Yonker
Stacey Strack

WRITERS
Brandyn Fisher
David Lefever

DISCLAIMER: *The information provided in this White Paper is strictly the perspective and opinion of The Mako Group, LLC and is not intended to protect an organization against a cyber attack, but mearly provide prospective on creating an information security plan. All content is owned by The Mako Group, LLC and is not to be reprinted or copied without experessed permission.*

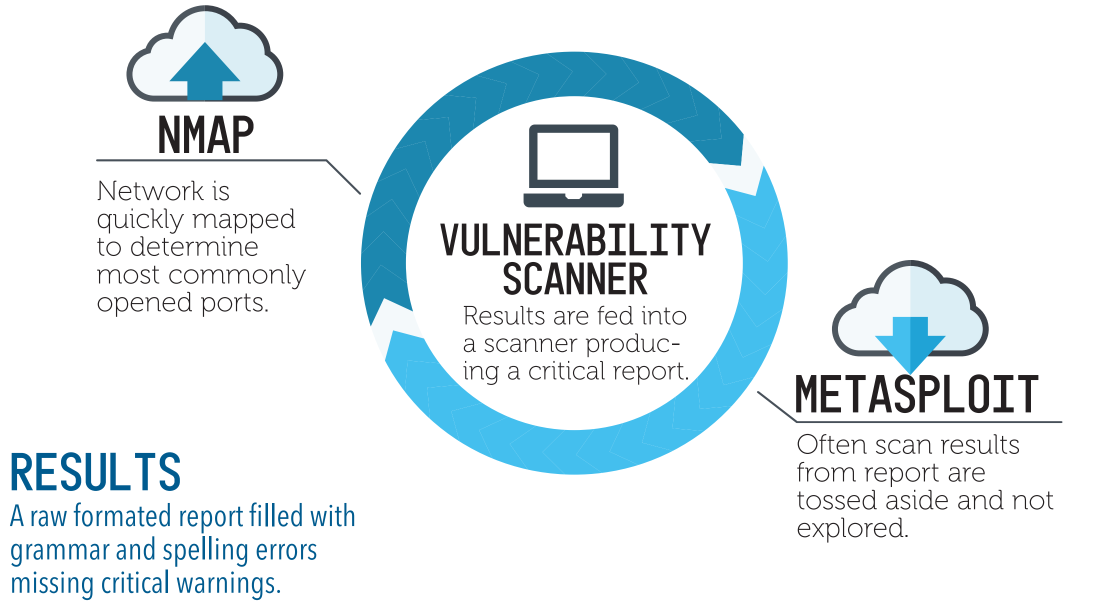
Being in charge of cybersecurity is a daunting task.

The role is largely maturing across multiple industries. You must rely heavily on internal teams, such as audit, technology and risk. Meanwhile, the media seems to focus on which organization was hacked and how it was hacked. It's a PR nightmare. As a CISO, the same thoughts may continuously consume your mind:

> *"If we have a breach, I'll lose my job. We'll end up all over the news. I think I'm doing enough, but am I? It doesn't matter how much we spend; it doesn't matter how many devices we buy – we can still get hacked. I just can't get peace of mind around whether or not we're secure enough."*

Over the past few years, many organizations have created temporary peace of mind through network testing and assurance through penetration tests. Afraid of landing in tomorrow's news headlines, organizations hire third parties to assess and test their network for vulnerabilities. While organizations understand the significance of a penetration test, they continue to select vendors with a heavy focus on a limited-scope or reduced investment. Below, we'll explain how to most effectively manage your network security risk, and attempt to reveal "how NOT to get hacked."

Common Network Testing



NMAP

Network is quickly mapped to determine most commonly opened ports.

VULNERABILITY SCANNER

Results are fed into a scanner producing a critical report.

METASPLOIT

Often scan results from report are tossed aside and not explored.

RESULTS

A raw formated report filled with grammar and spelling errors missing critical warnings.

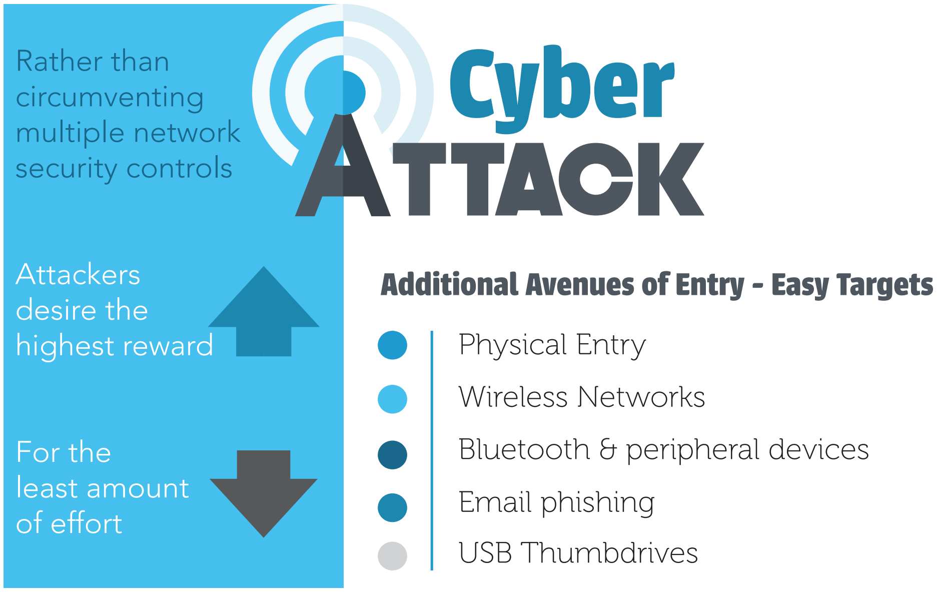
You Should Expect More

Breaking down the process

Organizations that fall victim to these routine penetration tests often find they are paying for a penetration test but receiving a vulnerability scan. The tools listed above are essential for performing a penetration test, especially under tight time constraints. However, these tools should not become a crutch for the assessment. There is no magic button that will fully automate a penetration test nor a magic scan that will provide the same level of thoroughness as a true penetration test. Penetration testing, by nature, requires the penetration tester to manually examine each vulnerability to identify the weakness and ascertain how it fits into the larger picture.

A different perspective

A symbiotic relationship exists between cybersecurity and malicious threat actors. As the skills, abilities and knowledge of threat actors increase, cybersecurity safeguards must be enhanced. This in turn forces threat actors to find new ways to circumvent new technologies and controls. Without this relationship, the cybersecurity field would become stagnant. Organizations should not assume an attacker will rely solely on network-based attacks for entry into their network.



Cyber ATTACK

Rather than circumventing multiple network security controls

Attackers desire the highest reward

For the least amount of effort

Additional Avenues of Entry - Easy Targets

- Physical Entry
- Wireless Networks
- Bluetooth & peripheral devices
- Email phishing
- USB Thumbdrives

A false sense of security

Organizations typically receive a report from their network security vendor with a laundry list of vulnerabilities, along with guidance that they will be protected from attacks upon correcting the vulnerabilities. In reality, this is almost never the case. A holistic penetration test must examine all the avenues in which an attacker may attempt to penetrate security defenses, not just network defenses. Threat actors look for the weakest point to attack, which is rarely your perimeter. Modern enterprise firewalls, if kept up to date, do a great job of protecting your network from the outside. But that makes no difference if your operating systems are not fully patched, as a threat actor could walk into your office unimpeded and boot a workstation from a USB thumb drive; or an attacker could trick users into providing their username and password over the phone. The scary part is that these scenarios are not difficult or uncommon.

What to look for

A mature assessment will focus on a full penetration test rather than a network only penetration test. A penetration test should be multifaceted and address all aspects of violating the confidentiality, integrity and availability of the organization's data and network. Organizations do not possess the luxury of limiting what a threat actor can and cannot attempt; therefore, they should include as many attack avenues as possible in their penetration test to fully understand and measure the organization's risks.

When reviewing the scope of a penetration test, consider the following targets that are commonly exploited by threat actors:

- Wireless Networks
- Bluetooth Devices
- Employees
- Mobile Devices
- I/O Devices
- Physical Devices

In addition, organizations should consider including the following types of assessments within the scope of an engagement with their third-party service provider:

- External Network Penetration
- Internal Network Penetration
- Wireless Penetration Testing
- Bluetooth Device Testing
- Email Phishing
- Voice Phishing (Vishing)
- Physical Social Engineering
- Web Application Testing
- Peripheral Device Testing
- Cyber Footprint Analysis

Raising the bar

Where there is money to be made, service providers will compete tooth and nail for your business. When selecting a security penetration testing vendor, it is crucial that organizations review the full gambit of work to be performed to ensure the penetration test is comprehensive. Vendors that market and sell vulnerability scans as penetration tests lower the perceived value by making penetration testing a commodity rather than a service.

Organizations should ensure their assessment is not dependent on a single set of tools and their service provider has the ability and skillset to utilize a large, customized set of tools. Just like a mechanic does not rely on a single socket wrench to repair a car, a penetration test should not rely on a single tool to assess the overall security of the organization. Tools should be carefully selected and customized based on the risk, as described below, to meet the individual need of the organization.

Network risk: An external and internal network penetration test, which should consist of more than just a few NMAP port scans, focuses on finding vulnerabilities on the network and methods of exploiting software and services on the various systems. Vulnerability scans assist in speeding up the discovery process, but can be riddled with false positives and negatives that must be investigated further during the exploitation and vulnerability confirmation phase of testing. Nonetheless, the most important aspect of any penetration test is information gathering, as it is instrumental to the outcome of subsequent testing phases. In addition, conducting an analysis of the organization's public footprint, which is the platform hackers use to obtain what they need to gain entry, is advisable and highly useful in ascertaining a complete picture of how the organization operates.

Web application risk: As technology has become an immensely vital part of the business world, the number of web applications has grown exponentially. Web application penetration testing attempts to violate security controls and program logic to access unauthorized parts of an application or perform actions not intended by the developer. It looks past the server on which the application resides and into the program or application being hosted. Short development cycles and complex application requirements have led to an increasingly high number of application vulnerabilities waiting to be exploited.

Wireless risk: Wireless testing assesses the security controls around the organization's WLAN. Often offered as a convenience to employees and visitors, WLANs provide an easy avenue for attackers to infiltrate the network without a physical presence, as it means attackers could be miles away and still access an organization's network resources.

Human capital risk: Vishing, email phishing and physical social engineering focus heavily on vulnerabilities in the workforce and assess employees' willingness to perform tasks that violate organizational policy. Human behavior is the most difficult vulnerability to remediate, which is why it's often the most exploited vulnerability. Through a few simple social tricks, it's possible to accomplish almost anything.

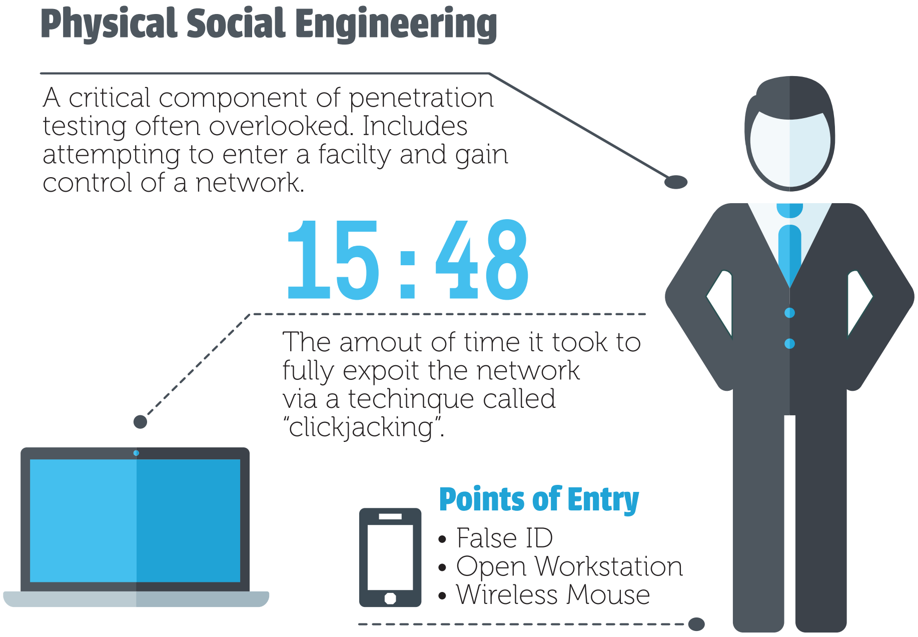
Peripheral device risk: Bluetooth and peripheral device testing are reserved for mature penetration tests, as they attempt to access information and systems through mobile and third-party devices, such as cell phones, headsets, mice and keyboards. Peripheral devices are often an afterthought during a penetration test and not regarded as legitimate attack avenues. Attackers hope for this line of thinking so they may skate by unnoticed in a single mouse-click.

A Real World MAKO Case Study

During a recent engagement with a major healthcare organization:

A full penetration test was performed over expansive attack avenues revealing that many servers were missing several third-party software and operating system patches on the internal network. Further exploitation of these vulnerabilities required access to the management VLAN, which was restricted to authorized devices via port security. Thus, the network portion of the penetration test did not enable access to the organization's network.

In sharp contrast, the physical social engineering portion of the penetration test allowed network access. The testing team was able to enter the facility under false pretense and reboot a workstation to Kali Linux from a USB thumb drive. From this point, locating password hashes and exploiting network vulnerabilities to obtain local administrator access on the network was trivial. To further illustrate weaknesses in the organization's environment, the testing team searched for wireless peripheral devices. In an attack known as "clickjacking," the testing team was able to create an account on a workstation by sending commands to a wireless mouse receiver. After escalating the account's privileges to domain administrator using the same attack tactic, the network was fully exploited.



Physical Social Engineering

A critical component of penetration testing often overlooked. Includes attempting to enter a facilty and gain control of a network.

15:48

The amout of time it took to fully expoit the network via a techinque called "clickjacking".

Points of Entry

- False ID
- Open Workstation
- Wireless Mouse

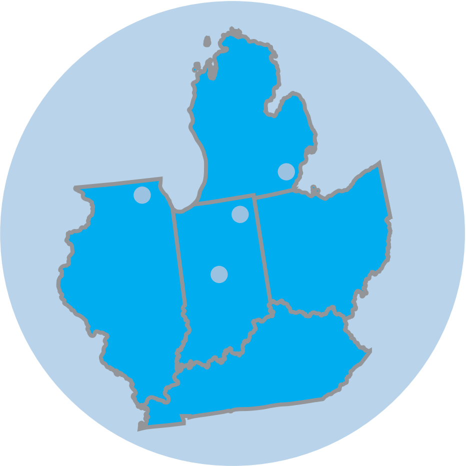
themakogroup

Security | Risk | Audit | Advisory

Who we are

The Mako Group is an audit, risk, security and advisory firm with offices in Chicago, Detroit, Fort Wayne and Indianapolis. We focus on you – on relationships, communication and impeccable deliverables. Everything we do is to achieve the highest level of security and audit standards, beyond the minimum requirements, for you. It's our gold standard. The Mako Group saves you time, hassle and a lot of money. We do this by providing quality work, using a combination of industry standards and best practices, and employing well-seasoned, senior-level staff. We do this because it makes you more secure. And because it just makes sense. Putting these standards in place is why we've never lost a client, and why we continue to grow using our client-first based service approach.

themakogroup



Contact Us: 877-247-MAKO (6256)

C

Chicago, Illinois
2011 W. Montrose Ave.
PO Box 135
Chicago, IL 60618
Email: chicago@makopro.com

D

Detroit, Michigan
19 Clifford St
Detroit, MI 48226
Email: detroit@makopro.com

F

Fort Wayne, Indiana
222 Pearl Street
Fort Wayne, IN 46802
Email: fortwayne@makopro.com

I

Indianapolis, Indiana
8555 River Road - Suite 320
Indianapolis, IN 46240
Email: indianapolis@makopro.com

D

Washington, DC
641 S Street NW
Washington, DC 20001
Email: washingtondc@makopro.com

www.makopro.com

The Mako Group
877-247-(MAKO)
contactus@makopro.com

How we help

The Mako Group offers a wide variety of professional services and develops an individualized approach for each client we serve. Our services include, but are not definitely not limited to:

Security

- Digital Footprint Analysis
- Network Configuration Analysis
- Network Penetration Testing
- Peripheral Testing
- Physical Entry Testing
- Security Program Development
- Social Engineering
- Web Application Testing
- Wireless Testing

Audit

- Agreed Upon Procedures
- Authorization to Operate (ATO)
- Control Design and Testing
- Control Mapping
- Framework Alignment
- Identity Access Management
- IT Audit
- MARS-E
- Model Audit Rule
- Operational Audit
- Sarbanes-Oxley (SOX)
- SOC Reports
- User Access Testing

Risk Assessments

- AML/BSA
- CSC 20
- ISO 27001/2
- FFIEC
- GLBA
- HIPAA
- IRS 1075
- NIST Cybersecurity Framework
- NIST 800-53 and 800-171

Consulting and Advisory

- Audit Preparedness
- Data Loss Prevention
- BCP & DR
- GDPR
- Governance, Risk & Compliance
- Incident Response Planning
- Cyber Maturity Models
- Policy & Procedure
- Risk Register Development
- RSA Archer GRC
- SAP GRC
- Security Programs
- Sourced CISO
- Supplier Risk Management
- System and Security Plans

Who we help

The Mako Group believes in partnerships with those we serve. While engagements are completed successfully, the partnership never truly ends. The Mako Group continues to work with clients where possible, long after our engagements have ended. Our client profile includes:

- Ally Financial
- Ashland Chemical
- Commonwealth of Kentucky
- Cooper Standard Automotive
- Dart Container (Solo Cup)
- Do it Best Corporation
- Franklin Electric
- Guardian Industries
- Indiana Pacers
- Intel Care Innovations
- Kite Realty Group
- Mayer Brown Law
- Parkview Health Systems
- RLI Insurance
- Sallie Mae
- Schlage Lock
- Tampa Bay Water

www.makopro.com

The Mako Group, LLC
877-247-(MAKO)
contactus@makopro.com