REAL SECURITY IS DIRTY

ROOK SECURITY

INFORMATION SECURITY AND RISK MANAGEMENT ARE PURSUITS OF BRUTAL SELF-REFLECTION.

THE MOST LOGICAL BUSINESS DECISIONS COME FROM FACING UGLY TRUTHS.

Before any business spends a dime on infosec or risk management, company leadership should start with honesty right from the get-go. Whether you're a line-of-business executive, a CIO or a CISO, ask yourself truthfully: How secure do you really want to be?

The knee-jerk reaction is usually, "Of course I want to be very secure!" But true security is far from a foregone conclusion. If they're being honest, many executives will admit that what they *really* want is to adhere to the legally acceptable minimum standard of security. Or they might admit they want to at least appear secure to customers.

If those are your answers to how secure you want your business to be, that is fine—it is even the norm today. But that means this e-book is probably not for you. There are plenty of compliance regimes and checklists out there already that can walk you down that path.

> THIS E-BOOK IS MEANT FOR THOSE WHO REALLY, TRULY WANT TO SECURE WHAT MATTERS MOST TO THEIR BUSINESSES.

If you are *serious* about IT security, you need to hear this message: It is time to stop being so prissy about how your security department analyzes your threats. Real security tests are messy. They take time. And they're not bound by hundreds of restrictions—because actual attackers aren't bound by rules, either.

The truth is that real security is dirty because dirty is the only path to honest assessment. And honest assessment is how businesses make better decisions about how to invest in protections that defend their highest value assets.

TODAY'S PENETRATION TESTS ARE LIES

Chances are you're probably lying to yourself and to your board about how secure you really are. They're not necessarily *intentional* lies, but they're lies nevertheless. And they're being told because the types of tests your business uses to assess weaknesses in technology and processes aren't nearly thorough enough.

Out in the world of security consulting, we run into a lot of business executives and even security executives who are aghast at the idea of a penetration tester taking a month to assess their clients' weak spots.

But here's the reality: One-day penetration tests aren't going to find out much about an organization's vulnerabilities. The same goes for tests that limit where penetration testers can go within certain buildings, what IT assets they can touch, which employees they can target and so on.

NOT EVERY PENETRATION TEST IS CREATED EQUAL.

A lack of industry standards has caused many tech service providers to market simpler tests as true 'penetration tests.' Here are some ways to distinguish the pretenders from the defenders:

	NOT REALLY A PEN TEST	NOT REALLY A PEN TEST	A TRUE PEN TEST
FEATURES	Automated scan that identifies network and application weaknesses	Automated scan, plus manual analysis to verify weaknesses	Advanced analysis of vulnerabilities that include pivoting and extending through a network and social engineering probes
DELIVERABLES	100-page listing of thousands of vulnerabilities with little remediation guidance	50-page report with vulnerabilities categorized into three to four criticality ratings, along with some remediation advice	Simple-to-understand report categorized with executive summary and methodology, along with prioritization of remediation based on business impact
MARKETED VALUE	Awareness of all potential internal/ external vulnerabilities	Awareness of technical vulnerability priorities, with remediation advice based on those	Awareness of business risk priorities, with remediation steps based on those
WHAT IT REALLY IS	VULNERABILITY SCAN	VULNERABILITY ASSESSMENT	PENETRATION TEST

Boards of directors, internal audit committees, CEOs and CFOs all trust their IT and security teams to honestly tell them how likely their organizations could be be successfully targeted and attacked by real-life bad guys. That kind of honesty requires penetration testers to go about their business very similarly to the way bad guys would. To be sure: The bad guys don't take a day to probe a target, and they certainly don't limit themselves to which assets or employees they go after.

Limited penetration tests offer a false sense of security. This is why one-day tests that throw infected thumb drives in the parking lot are actually worse than doing no test at all. They tell upper-level executives that everything is A-OK when they are not. As a result, they accept risk based on flawed assumptions.

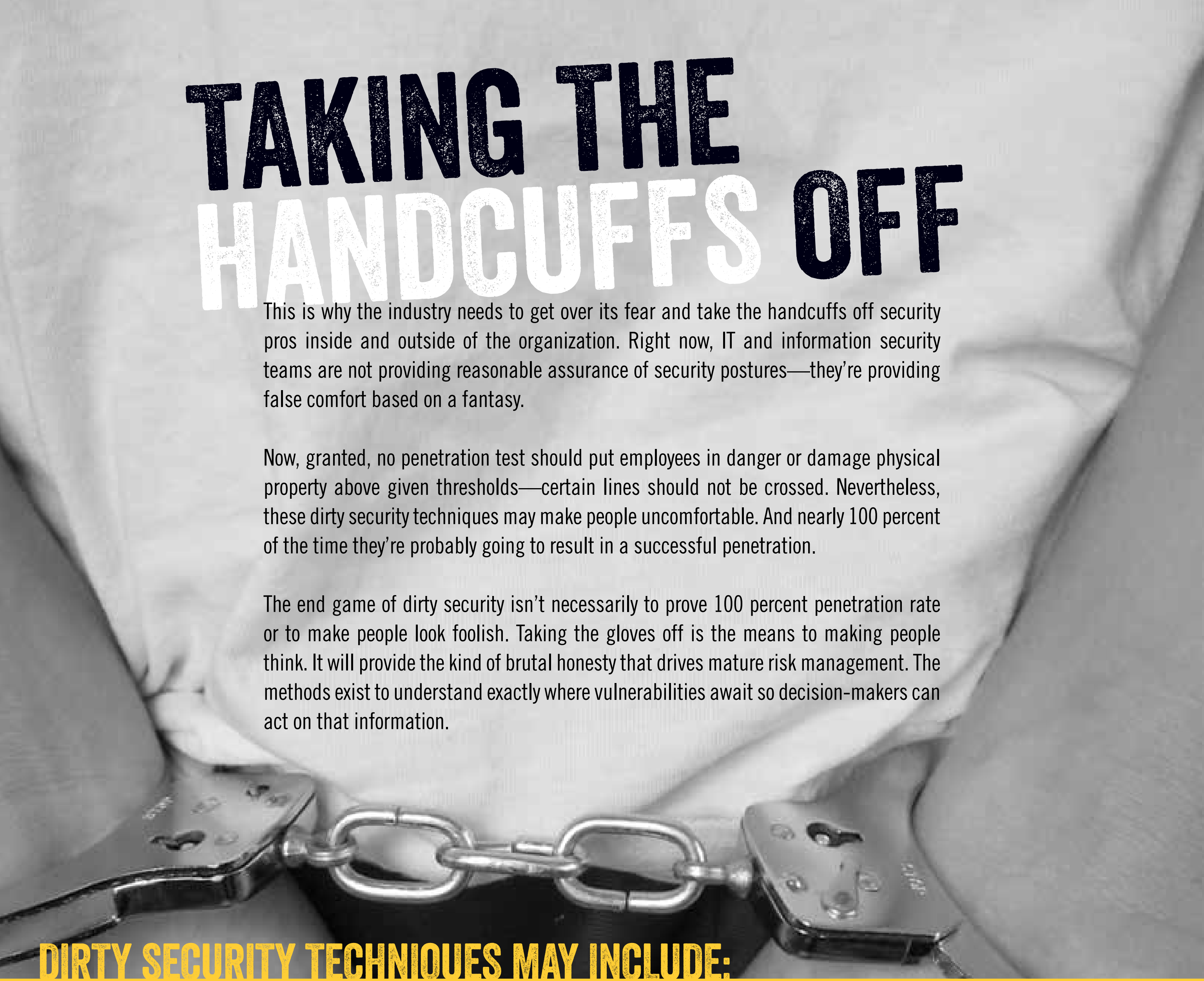
ATTACKERS FIGHT BELOW THE BELT

Attackers don't limit themselves to who they attack, when they attack or how they attack. For example, true story, we've witnessed manufacturing companies that have gone to great lengths to disguise prototype models that leave their R&D facility doors because spies with telephoto lenses might take pictures to steal their designs prior to launch. In infosec, dirty tactics they use include:

Standing up a fake access point near executive homes to identify porn sites, and gain access to social media and smart home systems.

Disrupting pacemakers or family medical devices while loved ones are in hospitals to blackmail executives into espionage participation.

Taking over a smart car or smart home system as a proof of power to gain similar cooperation for external insider attacks.



TAKING THE HANDCUFFS OFF

This is why the industry needs to get over its fear and take the handcuffs off security pros inside and outside of the organization. Right now, IT and information security teams are not providing reasonable assurance of security postures—they're providing false comfort based on a fantasy.

Now, granted, no penetration test should put employees in danger or damage physical property above given thresholds—certain lines should not be crossed. Nevertheless, these dirty security techniques may make people uncomfortable. And nearly 100 percent of the time they're probably going to result in a successful penetration.

The end game of dirty security isn't necessarily to prove 100 percent penetration rate or to make people look foolish. Taking the gloves off is the means to making people think. It will provide the kind of brutal honesty that drives mature risk management. The methods exist to understand exactly where vulnerabilities await so decision-makers can act on that information.

DIRTY SECURITY TECHNIQUES MAY INCLUDE:

- Mailing "contest-winning" interview requests based on social media interests
- Gaining employment on help desks, IT administration or janitorial staff for long-term data theft
- Utilizing dating sites or "chance" romantic encounters to gain corporate credentials

GETTING THE MOST OUT OF DIRTY SECURITY:

HERE'S WHAT A DIRTY SECURITY TEST MIGHT LOOK LIKE, BASED ON A REAL-LIFE ENGAGEMENT AT ROOK: In this particular example, our testers developed a special, homegrown badge-cloning device that could steal digital information wirelessly from RFID door keys. We were testing a high-tech company's data center, so we conducted online research ahead of time to find photos and information about key staffers who would be entering and leaving this high-value facility.

Our testers then hung around in the parking lot to spot those people and get close enough to clone their cards. From there, we used these clones to badge-in right after our targets so as not to arouse suspicion; instead, it would look like the person just badged-in twice.

We'd also performed reconnaissance about engineering team behavior and entered at a time when most of the team would be out of the office. At that point, it was trivial to enter the facility, locate hardware with sensitive data and leave with the hardware.

THE TAKEAWAY

Post-mortem analysis of the successful penetration and recommendations after the test is where the rubber meets the road for true risk posture improvements. Providing the right analysis of what went wrong and suggestions to move forward can be a delicate challenge, though.

Take the dirty penetration test in our example, above. The organization could have responded to the information about the incursion in several ways. They could have installed expensive network access control in the engineering lab, but that wouldn't have been financially feasible. So our recommendations laid out some simple and affordable risk mitigation measures, including making sure people are not sitting around in cars in high-value facility parking lots, improving badge verification processes and updating badge technology so that it is less susceptible to cloning.

The point of all of this is that this company would never have even known about the issue or these potential remedies if the penetration test hadn't been allowed near that high-value facility. This is why dirty security is so important. It provides valuable knowledge. And it lets business leaders accept or mitigate risks based on nothing but the truth.

ROOK™ SECURITY

888.712.9531

info@rooksecurity.com
rooksecurity.com
facebook.com/rookconsulting
linkedin.com/company/rook-security
twitter.com/rooksecurity