ARMOR™

BETWEEN YOU AND THE THREAT

Defending inside out

COMBAT THE INFINITE INSIDER THREATS | ARCHITECT VANTAGE POINT

CHRIS HINKLEY | **SR. SECURITY ARCHITECT | ARMOR**

The forgotten attack vector

It's the forgotten attack vector. The lackadaisical worker. The disgruntled employee. A staffer lured by dollars. The nefarious vendor or contractor. Or even a trusted worker extorted or manipulated against their will.

The reasons employees create security vulnerabilities or turn to illegal craft are untold and numerous. But the threat is real — and it needs to be defended against with diligence and persistence.

> "While outsiders will always be a concern, some of the greatest risk may come from your own employees."
>
> CHRIS HINKLEY
> SR. SECURITY ARCHITECT | ARMOR

What's real, what's fiction

When you envision the threats facing your company, there's a natural tendency to imagine malicious hackers and organized cybercrime rings.

No doubt the lion's share of your security budget is devoted to protecting your data from outside threats. Yet while outsiders will always be a concern, some of the greatest risk may come from your own employees.

We're not necessarily talking about employees who deliberately misuse privileges and steal your data (though that does happen). The more common scenario is the security threat posed by employees who unknowingly violate your security policies and procedures every day and go unchecked. Often, they have no idea of the threat they represent to your organization and its infrastructure.

Yet these employees can often be your greatest risk, whether they're creating unsafe work practices or are simply naïve about social engineering and other potentially dangerous actions.

Insider threats: They can happen to you

Think it can't happen? Recently, the South Carolina Department of Revenue's website was hacked when an employee opened a malicious file after being duped by a social engineering tactic. As a result, more than 3 million social security numbers were stolen.

Remember, most of your employees aren't aware of the latest criminal methodologies. They could download non-secure apps on their company laptops, visit a maliciously infected website or decide to use software that doesn't meet your internal security standards.

Threat actors and malicious criminal organizations understand this lack of education as well. If they aren't successful at compromising the identities of an employee via malware or social engineering, they'll target your vendors or other third parties who have similar access.

They'll refocus their attempts on these groups, prodding for security gaps, vulnerable systems or applications, and irresponsible employees.

The possibilities are almost endless — which is why so many hackers enter the network through your own workforce.

Looking Inside

Internal security threats may take any number of shapes or forms.

- Sharing credentials for logical or physical access
- Document or IP theft
- File manipulation or falsification
- Code or software alteration
- Installation of malware through phishing or fraudulent websites
- Use of unknown or non-secure USB drives
- Apathy around security policy, especially in regards to software, phishing, social engineering, etc.

Develop your plan

When developing a security plan, it's just as critical to guard your company from inside threats as it is to defend it from outside dangers. Security and compliance are about people, processes and technology.

Investing in security expertise and best-of-breed technology is great, but your risk management program must account for the employee risk factor. If it doesn't, the side door is left unlocked. No doubt your internal security controls already include a variety of monitoring, alerts and forensic data in order to protect your perimeter — but it's still a good idea to ensure your internal safeguards.

Keep security & computer use policies updated

Clearly outline protocol around data confidentiality and electronic media usage. Every employee must understand the rules and reasons for them.

Host recurring security training sessions

Many employees will disregard policies when they don't understand the risk at stake. Explain the company repercussions of breaking security policies and encourage employees to come forward with any needs. This transparent approach is preferred over employees attempting to download apps or creating new processes themselves.

Know what tools & applications your employees are using

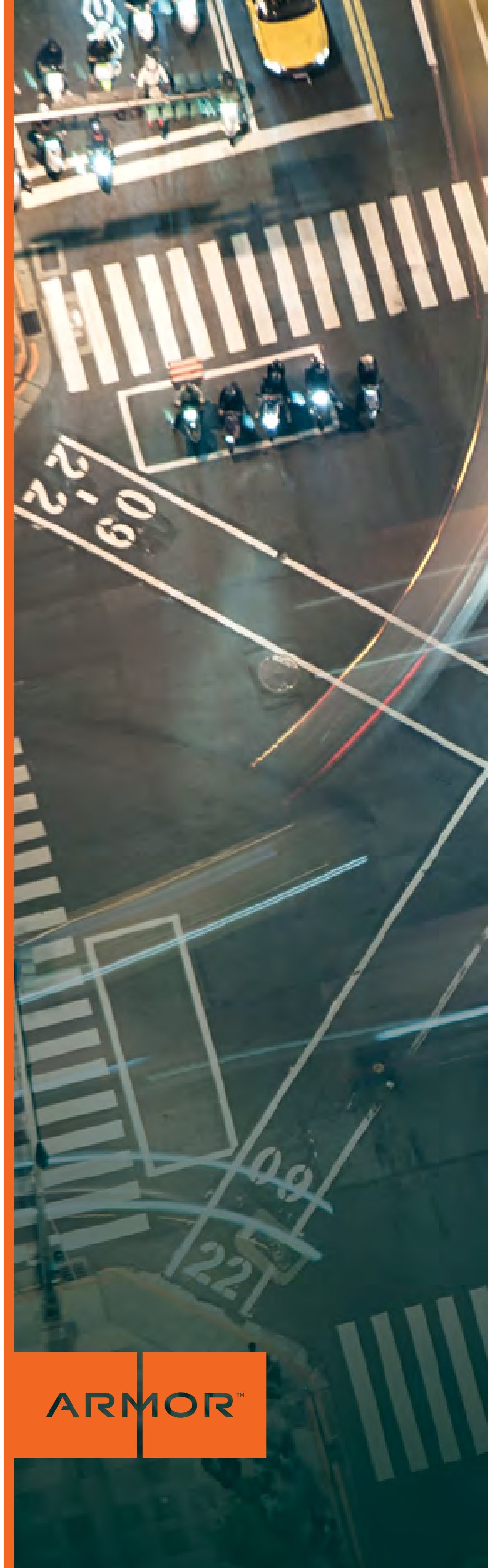
You can't fully assess risk if you don't know the tools your employees are using (e.g., Dropbox and Google Drive) on their company-issued computer. Investigate the ratio of unapproved services to approved services used by your workforce and you'll have a more accurate idea of your vulnerability.

Practice vigilant asset management

This sounds like a no-brainer, but it's a weak spot in many organizations. Always know what you have, where it is, who can access it and how it's vulnerable. Eventually smart phones and laptops will get lost or stolen, so create a security plan for that event.

Protect yourself against employee risk

Have a system in place to access, audit and review employee systems for updates, and utilize good antivirus software. To mitigate damage from stolen credentials, draft and enforce password resets regularly. Finally, filter employee Web traffic through a proxy, so you have the ability to monitor and block access to known bad domains.



Persistence is key

After developing solid controls for insider threats, be sure that your internal and external safeguards are working seamlessly together. As we all know too well, attackers will detect and exploit any existing gaps.

> "Turn your security sights inward and make sure your best assets **— your workforce —** aren't also your greatest vulnerability.
>
> **Educate them.**
> **Protect them.**
> **Empower them.**"

About Chris Hinkley

As senior security architect at Armor, Chris Hinkley utilizes a decade of security expertise to design, test and deploy next-generation security processes and techniques for the cloud. His work at Armor was instrumental in Armor being one of the first cloud companies globally to achieve PCI DSS compliance.

Prior to Armor, Hinkley worked as a Web developer for TargetScope, an interactive marketing and Web development company. In that role, Hinkley created everything from website animations to complex and dynamic product configurations using the latest technology and development frameworks.

With Armor, Hinkley has held a number of security and technology-related roles, including security engineer, lead engineer and support manager. He has serviced thousands of Armor customer servers and overseen the security of all hosting environments to meet PCI, HIPAA and other compliance guidelines.

Hinkley is a sought after speaker and author on cloud, security and open source topics, publishing regular columns in SecurityWeek and other industry magazines. Hinkley is a Certified Information Systems Security Professional (CISSP).

US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™

BETWEEN YOU AND THE THREAT