Insider Threats Survey

Fielded April 2011

threatpost

The Kaspersky Lab Security News Service

Executive Summary

Paul Roberts, Editor, Threatpost

The Enemy Within: Enterprises Ill Prepared for Insider Attacks

A Threatpost survey of 105 enterprise users reveals the emerging threat of attack from trusted employees and the inconsistent ways companies are fighting back.

Modern businesses thrive on increased collaboration and information sharing. As a result, today's enterprises are granting employees of all levels access to a growing number of network resources, enterprise applications and other sensitive IT assets as a way to promote greater worker efficiency and improved business performance. But there's a downside.

A new survey from Threatpost shows that companies are increasingly under attack from within; victims of the very workers they've entrusted with broader access to vital systems. As Threatpost has reported previously, malicious insiders are a persistent and growing problem in the halls of government as well as in companies of all sizes. (http://threatpost.com/en_us/slideshow/infamous-insiders-10-eye-popping-heists-insiders/insider-threats) Moreover, most enterprises remain woefully unready to prevent, detect and mange such insider attacks.

According to the new Insider Threats survey, one third of businesses polled – 32% – say a current or former employee has attacked their company's technology systems. Some 31% of those attacks came not from disgruntled workers or known troublemakers, but rather from current employees with clean personnel records. As security specialists turn their focus inward in response, it's important to note that most attackers had average, unremarkable technology skills and simply used the access and permissions legitimately granted them by corporate IT. Just 26% had raised their own permissions to administrator or root access without authorization.

A small but troubling 15% of reported attackers were members of the company's IT security team.

As in any security scenario, when crafting defenses, it's important to understand motive. According to the survey, attacks by insiders focus more on harassment and disrupting the business than on stealing money or intellectual property. Nearly 60% of insider attacks involved moving, deleting or altering access to corporate data; just 24% resulted in the theft of company funds or trade secrets. The vast majority – 43% – of those reporting internal attacks say the breach cost the company $25,000 or less, the Threatpost survey found.

Threatpost readers tell us:

Every company experiences these hits, the WWW, browsers, OS are not secure and cannot be secured, MS has been patching for what 20 yrs, never had a secure OS, even with the many good security vendors making a living trying to secure OS, priorities are on bells and whistles, not security.

Keep an open policy with everyone so information will be given by individuals without any kind of identity of the person relating the info

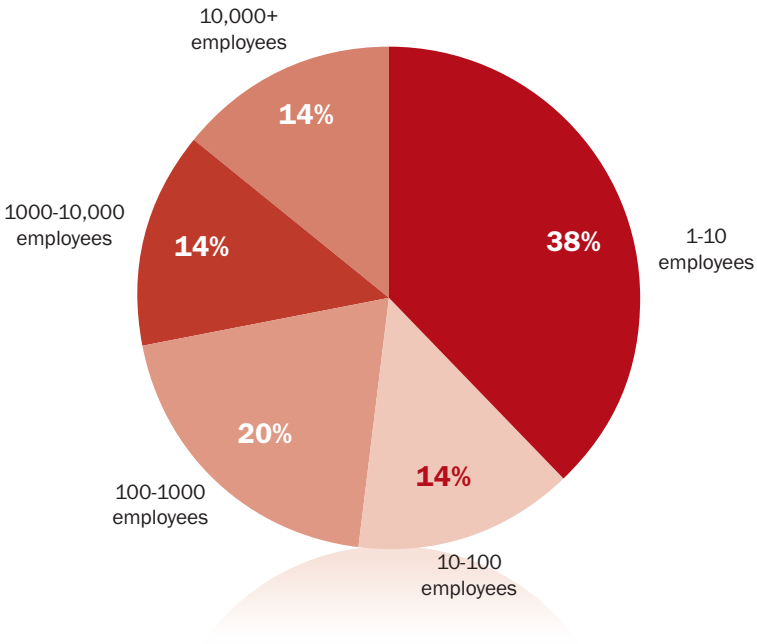
The issue is the copying of IP, we have taken steps to install DLP and monitor the access and keep track of the data once copied.

Given the pervasiveness of such internal attacks, corporate IT would be wise to step up defenses and enforcement. To date, however, their efforts appear lacking. 59% of internal cyberattacks are never reported to law enforcement or government regulatory agencies. In cases where law enforcement is notified, the investigations result in successful prosecution of the attackers in just 13% of cases. Threatpost has pointed out in the past the importance of forging better relationships with authorities and working more closely with law enforcement in the wake of an insider attack in order to improve such results. (http://threatpost.com/en_us/blogs/how-work-law-enforcement-after-attack-021511)

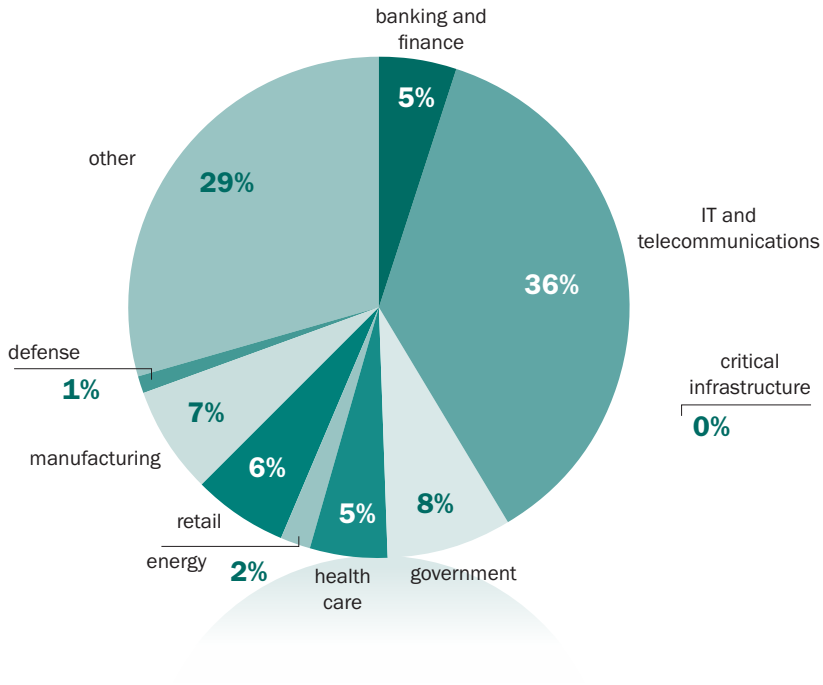
Check out Threatpost's Insider Threats Survey to see all of the ways attacks from within are vexing the enterprise and where IT security efforts need to be improved.

Insider Threats Survey Results

The size of my company is:



My company operates in the following industry:



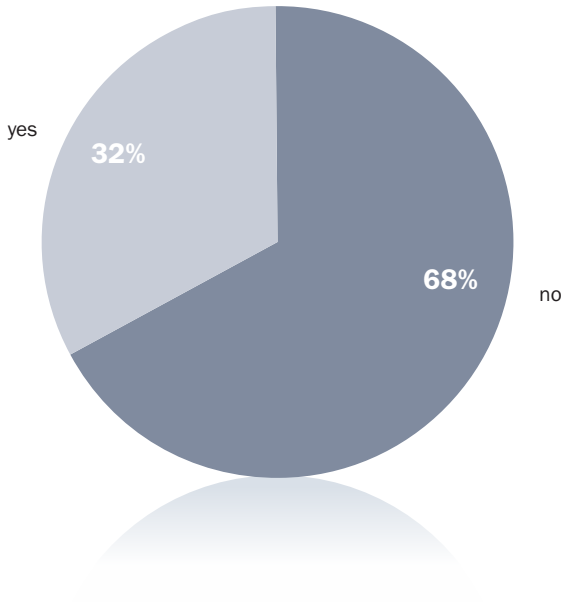
Threatpost readers tell us:

My company has not had any internal threat attacks. The employee who mentioned a desire to create problems was reported by co-workers and terminated from the company before any action was taken by the employee against the company systems.

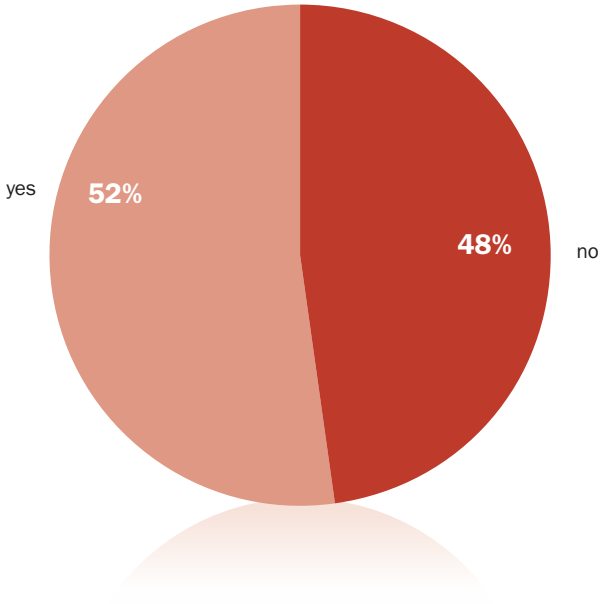
We did have an employee (later caught and fired) who installed a conficker version purposely to limit network access.

As an IT Security Consultant, I worry most about company Management incidents and a lot less in regards to IT security employees!

My company [ ] has [ ] has not previously been the victim of a malicious action by a current or former employee.

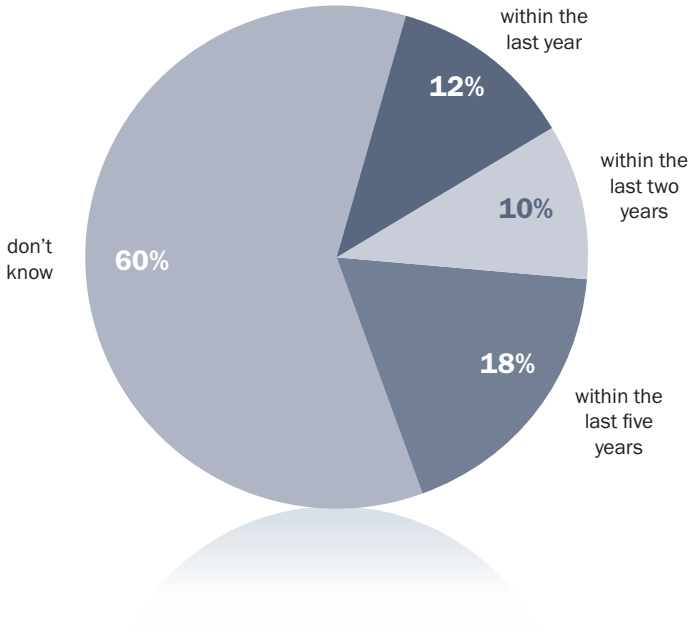


My company [ ] has [ ] has not previously been the victim of a malicious action by a an unknown assailant.

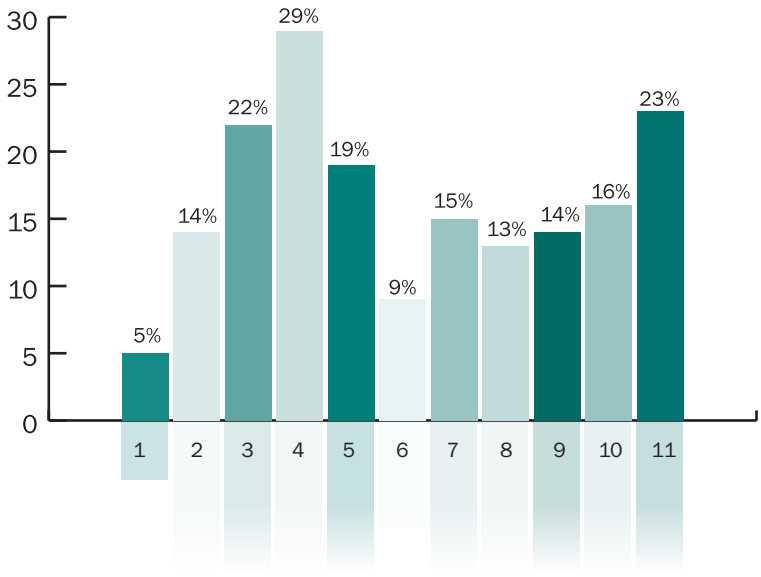


As is often true in security, the perpetrator is the person you'd least suspect. Only 13% of attackers gave any warning at all that they were planning to embarrass or retaliate against their employer. Those reporting insider attacks in our survey say they often fell victim to current employees in good standing with no known technical skills beyond average. That lack of technical sophistication is reflected in the kinds of mayhem insider attackers typically commit. Only 5% attempted Web site defacements and just 9% managed to steal money. Conversely, 29% simply deleted company data, while 22% installed Trojans or other malicious software.

My company has been the victim of an attack by a current or former employee at least once:



The following characteristics describe the incident(s) of malicious attack by a current or former employee against my employer:



1 Organization Web site was defaced

2 Access permissions to company assets were deleted or altered

3 Malicious programs or Trojan horse programs were installed on company assets

4 Data was deleted or moved

5 Customers or business partners were contacted

6 Company funds or assets were stolen

7 Intellectual property or trade secrets were stolen or deleted

8 Accounts or assets belonging to individual employees were targeted

9 Individual employees were harassed

10 Employees were denied access to company assets or network resources

11 Other

1 They were a current employee in good standing at the company at the time of the attack

2 They were a current employee, but not in good standing (had a record of disciplinary action, on probation or the subject of one or more grievances) at the time of the attack.

3 They were no longer employed by my company at the time of the attack.

4 Had communicated negative feelings about the organization to others prior to the attack.

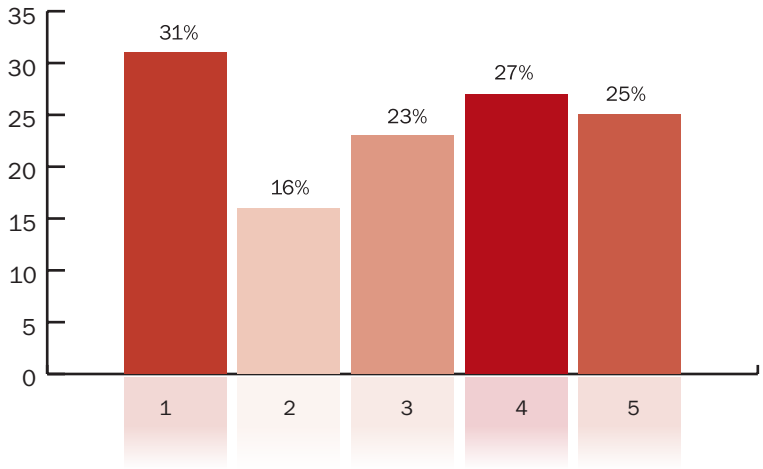
5 Other

Threatpost readers tell us:

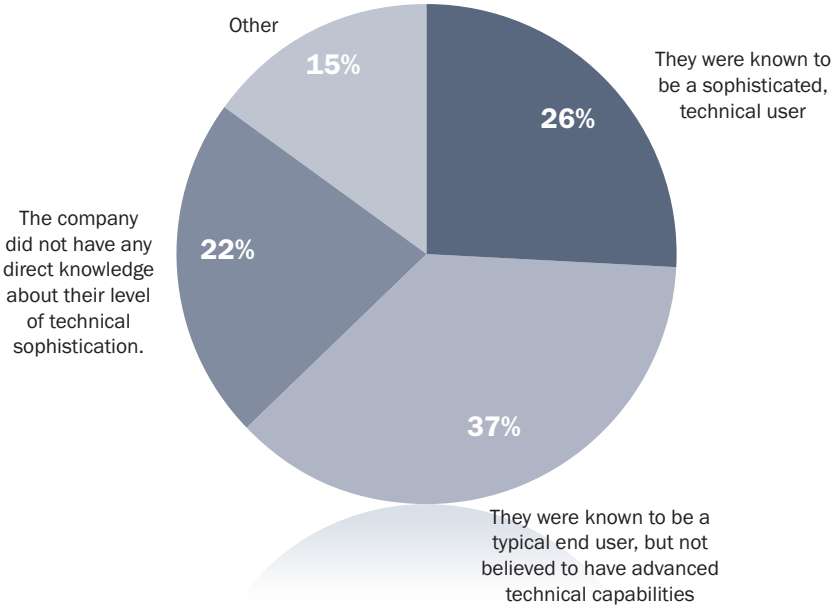
The hacker didn't do any real damage and we got control of the website and had it back up and running in a day. He was our lead webmaster so he had all the tools and skills needed to do this. Afterwards we never put the webmasters name on the ICAN records only the company names.

Balancing security risks and the benefits of an openness to the business is a difficult task indeed.

The following characteristics describe the insider(s) believed to be responsible for the attack:



The following characteristics describe the insider(s) believed to be responsible for the attack:



1 They were or had been a member of the company's IT security team, or had responsibilities that included computer security.

2 They had legitimate, user-level access to network and system resources at the time of the attack, but had elevated their privileges illegally to obtain administrator or root access.

3 They had legitimate, privileged (administrator or root) access to network and system resources at the time of the attack.

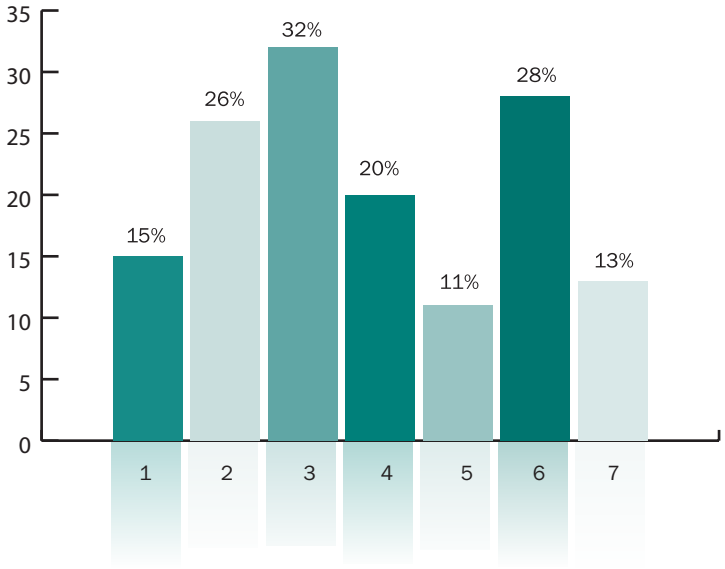
4 They had privileged access to network and system resources terminated at the time of the attack.

5 They had been terminated or left, but privileged access to network and system resources had not yet been terminated at the time of the attack.

6 Had communicated negative feelings about the organization to others prior to the attack.

7 Had mentioned plans to harm, embarrass or retaliate against the company or specific employees prior to the attack.

The following characteristics describe the level of access of insider(s) believed to be responsible for the attack:

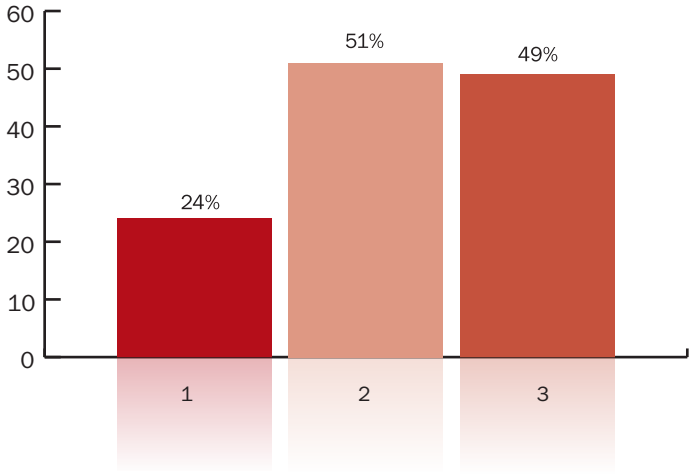


1 They took steps to lay the groundwork for the attack prior to carrying it out.

2 They took steps to conceal their activities and identity during and after the attack

3 They did not take steps to conceal their role in the attack after it was carried out

The following characteristics describe behaviors of the individual(s) believed to be responsible for the attack:



1 After being notified by customers or business partners of irregularities

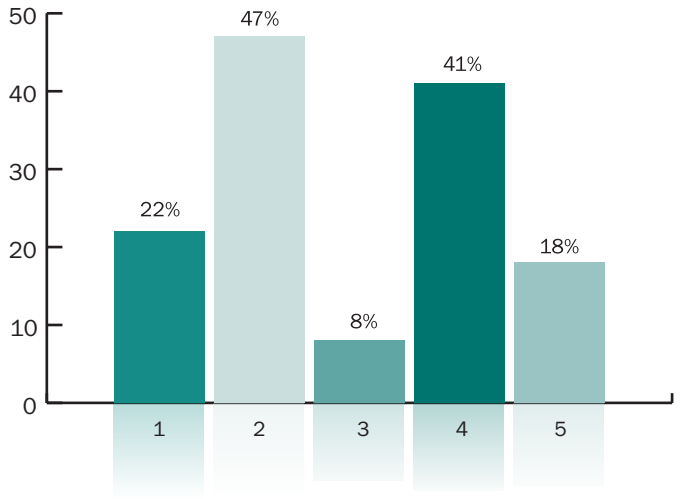
2 After being notified by employees and coworkers

3 After being notified by law enforcement or another official body (i.e. U.S. CERT)

4 After IT staff (internal or consultants) noticed irregularities in information or systems, including system logs, intrusion detection systems, file access logs, database or application logs, or phone records.

5 Other

In the incident(s) of insider attacks my company became aware of the attack.



1 Local law enforcement was notified.

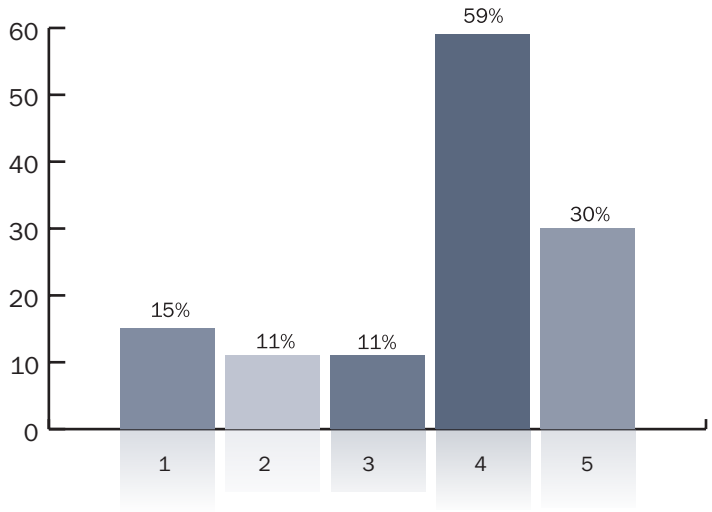
2 State or federal law enforcement was notified.

3 Regulators were notified

4 Nobody outside the company was notified

5 Not applicable

After the breach:



1 Authorities investigated and were able to link the attacks to a specific individual(s) and pursue criminal action against them.

2 Authorities investigated, but were not able to link the attacks to specific individual(s) or pursue criminal action against them.

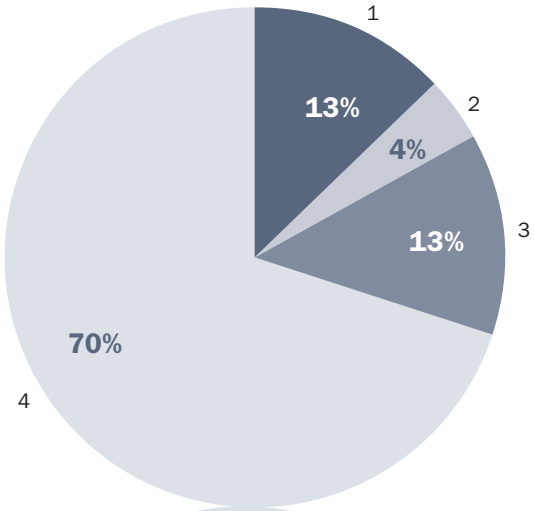
3 Authorities took no action to investigate the incident(s).

4 Not applicable

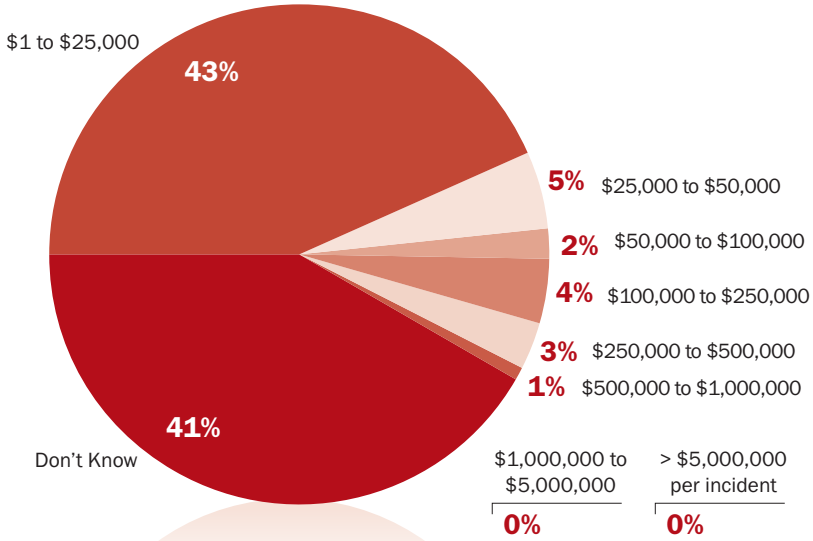
Determining the real damage from an insider attack can be difficult.

While 43% of those surveyed said the breach cost the company less than $25,000 – and another 41% couldn't estimate losses – a review of the way such attacks were discovers shows the intangible costs can be much greater. 30% of incidents were reported by customers, business partners, law enforcement or regulatory officials. Such exposure of security shortcomings to third parties can cause lasting damage to brand and reputation.

In cases where law enforcement was notified



The amount of damage to my company from these insider attack(s) per incident in the year(s) in which they occurred was



We hope you found Threatpost's Insider Threats Survey informative.
Read Threatpost daily to stay current on security issues affecting businesses today.