CYBERSECURITY VENTURES

Black Hat Employees Fuel Multi-Billion Market for UAM Solutions

Insider threat: CISOs biggest challenge? Latest statistical data heightens concern around employees and contractors.

Steve Morgan
Founder and Editor-in-Chief at Cybersecurity Ventures

Black Hat Employees Fuel Multi-Billion Market for UAM Solutions

Threats from insiders pose a huge cybersecurity risk to organizations today.

More than external threats, the prospect of malicious or negligent insiders deliberately or inadvertently harming an enterprise keep many a security practitioner awake at night. Insider threats can come from current and former employees, contractors, business associates, and just about anyone with inside information about an organization's inner workings.

Cybersecurity Ventures predicts that security risks posed by insiders is fueling rapid growth of UAM (user activity monitoring) solutions, and that market will reach $5 billion by 2025. Various estimates put UAM market growth at up to 25 percent annually over the next 5 years.

Despite the growing market, many businesses are reluctant to proactively search for such solutions until they experience the first real breach from the inside, according to Dennis Turpitka, CEO at Ekran System, a UAM, PAM (privileged access management), and IAM (identity and access management) vendor based in San Antonio, Texas. Various statistical analyses of the insider threat help put the overall risk into perspective.

BY THE NUMBERS

The editors at Cybersecurity Ventures have been following these facts, figures, predictions, and statistics on the insider threat:

- 90 percent of organizations feel vulnerable to insider attacks, whether malicious or not — and 53 percent of organizations have reported an insider attack in their organization during the past 12 months, writes Niv Goldenberg, a principal product manager for cloud application security at Microsoft.
- 28 percent of all cyberattacks are launched by malicious insiders, according to the latest Verizon Data Breach Investigations Report (DBIR). That doesn't include unintentional insider attacks, where an employee performs an act — such as opening an infected file — that leads to a data breach.
- A PwC audit committee update on the insider threat stated 90 percent of "insiders" displayed no worrying characteristics prior to their (cyber) attacks.
- The U.S. State of Cybercrime Survey found that 16 percent of those asked committed their crime for financial gain, and 10 percent for revenge.
- According to the 2018 IBM X-Force Threat Intelligence Index, 60 percent of all cyberattacks in the prior year were attributable to insider threats — those caused (intentionally or inadvertently) by employees and leaders within an organization — which are among the costliest and hardest to detect of all data breaches.
- Gartner reported last spring client inquiries about insider threat detection increased 50 percent over the previous year. "Our clients are seeking

solutions — both technical and non-technical — for a problem that legacy solutions are not effectively addressing," noted security analyst Avivah Litan.

- In Healthcare, 24 percent of cyberattacks are due to insider misuse — and for 13 percent of those type, employees attributed the breach to "curiosity" — for example, if a celebrity had recently been a patient, according to a story in Becker's Health IT & CIO Report.
- Nearly 53 percent of insider fraud incidents within the healthcare sector involve the theft of customer data, while more than 37 percent of the incidents targeted financial assets, according to CMU SEI (Carnegie Mellon University Software Engineering Institute).
- More than a third of insider incidents in IT organizations involve sabotage, according to the CERT Insider Threat Incident Corpus.
- CMU SEI reports that two-thirds of malicious insiders in the IT industry were with their companies less than a year. Almost half of them were in their thirties when they sabotaged their company.
- According to the 2019 Verizon Mobile Security Index, five out of six respondents said that their organization was at risk from mobile threats — and 29 percent said it was a significant risk.
- The White House's new National Strategy for Aviation Security calls attention to a rising concern in aviation safety: the potential for cyberattacks on aircraft, putting malicious cyber actors first on a list that includes malicious use of unmanned aircraft, insider threats, and other non-traditional aviation threats.
- Tesla has sued an employee it claims "unlawfully hacked the company's confidential and trade secret information and transferred that information to third parties" for $167 million.
- Punjab National Bank, India's second largest financial institution, last year claimed two junior officials at one of its branches used their access to the global payments network SWIFT to defraud the bank of $1.77 billion.

EXPERTS WARN ON INSIDERS

The insider threat is the number one security challenge for hospitals, according to Kathy Hughes, CISO at Northwell Health, which employs over 68,000 healthcare professionals, making the non-profit New York state's largest private employer.
"For far too long data breaches and cybersecurity incidents caused by insiders have been pushed aside and not taken seriously," states Bryan Sartin, executive director, security professional services, Verizon, in a recent article on the company's website. "This has to change. Cyber threats do not just originate from external sources, and to fight cybercrime in its entirety we also need to focus on the threats that lie within an organization's walls."

A MeriTalk story reports that Bill Evanina, director of the National Counterintelligence and Security Center (NCSC) in the Office of the Director of National Intelligence, stated that the billions of dollars the U.S. government and private sector spend each year on cybersecurity are not being properly and efficiently utilized unless government and industry wrap human resources departments tightly into security discussions. Evanina, speaking at an event hosted by Nextgov and Equifax, argued that HR represents an essential element in combating insider threats — which he called the biggest concern in nation-state espionage and theft of government and private sector proprietary data.

BLACK HAT EMPLOYEES

“One of the reasons why insider threats are so hard to detect is that insiders usually have the ability to cover their tracks,” says Ekran’s Turpitka. “After one successful uncovered attack, an insider can even consider such activity to be a part of the ‘normal’ opportunities he or she has at work.” Training white hat employees on cybersecurity doesn’t address the black hat employees. Turpitka concurs, and adds, “Inadvertent insiders can also be a constant risk source while their risky activity patterns are not detected and properly addressed. Security awareness, while helping to educate the uninformed, does not address the inadvertent threat.”

- Dennis Turpitka
CEO and Founder at Ekran System®

“Everyone in the world of cyber talks about ‘Black Hat Hackers’ but Cybersecurity Ventures has coined a new term — ‘Black Hat Employees’,” says Scott Schober, author of the popular book Hacked Again, and CEO at Berkeley Varitronics Systems. “This coveys a different angle in that the Black Hat is an employee on the payroll and they are maliciously getting into the computer network and covering their tracks,” says Schober, who frequently appears on TV as a guest cybersecurity expert. “As a business owner, I ask myself are there any employees that are insider threats? And now I ask myself an additional question — Are there any Black Hat Employees? Traditional Black Hats often have no connection to the company they are hacking.”

- Scott Schober
CEO/Berkeley Varitronics Systems, Speaker & Cyber security subject matter expert, Author of Hacked Again

One popular cybersecurity metric is “dwell time” — the duration a cybercriminal has undetected access in a network until they are completely removed. The average dwell time can be as long as 150 days, according to various sources.

If you consider that employees and contractors are permanent residents inside your network, then you had better be watching them.

Written by:
- **Steve Morgan is founder and Editor-in-Chief at Cybersecurity Ventures.**

Go here to read all of my blogs and articles covering cybersecurity. Go here to send me story tips, feedback and suggestions.