Office of Research Security Newsletter

September 2019

Insider Threat Detection a Serious Problem for U.S. Businesses

by Flip Truta June 24, 2019

Preventative security technologies like firewalls and application blacklisting aren't always enough to safeguard an organization's IT infrastructure. Businesses often face internal threats, so a cybersecurity strategy must include tools and processes for rapid detection and response. However, strategies often don't.

Ponemon Institute recently surveyed 627 IT and IT security practitioners in the United States to understand how organizations are addressing cyber risks associated with insider threats – such as negligent or malicious employees.

The overall findings paint a worrisome picture — organizations lack deep understanding of the risks of this type of threat. Respondents also revealed they are underprepared for resident attackers, and that they have little ability to discover and remove internal threats.

To read the full article –
https://securityboulevard.com/2019/07/insider-threat-detection-a-serious-problem-for-u-s-businesses/?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

REFRESHER SECURITY TRAININGS FOR 2019:

Thursday, Apr 25, BJA, RSA – 11:00 am to 12:30 pm

Tuesday, Jun 4, BJA, RSA – 11:30 am to 1:00 pm

Wednesday, Jun 19, OKT S105 – 11:00 am to 12:30 pm

Wednesday, Jul 17, OKT S105 – 11:00 am to 12:30 pm

Friday, Aug 2, OKT S 105 – 11:00 am to 12:30 pm

Thursday, Aug 29, BJA, RSA – 11:30 am to 1:00 pm

Thursday, Oct 24, BJA RSA – 11:30 am to 1:00 pm

- November Movie Month - VBH, M50 - 1:00 pm to 3:30 pm
- Tuesday, November 5, 2019
- Tuesday, November 12, 2019
- Thursday, November 21, 2019
- Monday, November 25, 2019

Security Clearance Backlog Drops By Nearly 40%

Attention is shifting to processing times and rolling out continuous evaluation to the entire clearance population. ***Government Executive, June 2019, by Lindy Kyzer***

The National Background Investigations Bureau can be proud of reaching a milestone many didn't think would be possible—reducing a 710,000+ backlog of pending investigations by nearly 40% and within reach of a steady state in less than a year.

The Performance Accountability Council released its cross-agency priority (CAP) goals update last week. Among the highlights are the reduction in the backlog and advancements in eAdjudication and personnel vetting—and NBIB's backlog busting investigation figures.

Officials with the Office of the Director of National Intelligence have previously stated that phase one of the security clearance reform effort was targeted toward the backlog. Now the focus turns to revamping the policy, updating the IT framework, and making continuous evaluation a reality.

To read the full article –
https://www.govexec.com/defense/2019/06/security-clearance-backlog-drops-nearly-40/158072/

OFFICE OF RESEARCH SECURITY STAFF

·DENISE SPILLER, SECURITY ADMINISTRATOR

824-6444 / denise.spiller@uah.edu

·JANINE WILISON, ASSOCIATE SECURITY ADMINISTRATOR

824-3025 / janine.wilson@uah.edu

·APRIL MCMEANS, ASSISTANT SECURITY ADMINISTRATOR

824-6048 / april.mcmeans@uah.edu

OFFICE OF RESEARCH SECURITY STAFF Continued

·CAITLYN SCHOENIG, SECURITY ASSISTANT

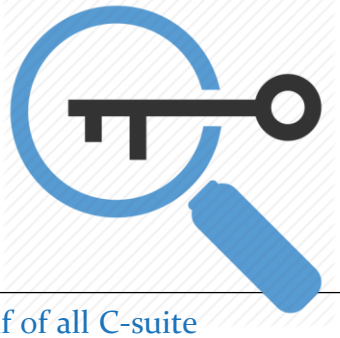
824-4717 / cns0017@uah.edu

·MARIAH WILKINSON, STUDENT SPECIALIST II

824-4818 / mw0077@uah.edu

Human error still the cause of many data breaches

HelpNet Security, June 17, 2019



With the incidence of reported data breaches on the rise, more than half of all C-suite executives (C-Suites) (53%) and nearly three in 10 Small Business Owners (SBOs) (28%) who suffered a breach reveal that human error or accidental loss by an external vendor/source was the cause of the data breach, according to a Shred-it survey conducted by Ipsos.

When assessing additional causes of data breaches, the report found that nearly half of all C-Suites (47%) and one in three SBOs (31%) say human error or accidental loss by an employee/insider was the cause.

What's more, one in five C-Suites (21%) and nearly one in three SBOs (28%) admit deliberate theft or sabotage by an employee/insider was the cause of the data breach, compared to two in five C-Suites (43%) and one in three SBOs (31%) who say deliberate theft or sabotage by an external vendor/source caused their organization to suffer a data breach..

"For the second consecutive year, employee negligence and collaboration with external vendors continues to threaten the information security of U.S. businesses," said Ann Nickolas, Senior Vice President, Stericycle, the provider of Shred-it information security solutions.

To read the full article - https://www.helpnetsecurity.com/2019/06/17/human-error-data-breach/?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE