NORTHERN NEVADA ASIS INTERNATIONAL
CHAPTER #164

May 4th 2016
Volume 6, Issue 7

Security Vanguard

Mark Crosby, CPP

Chairman's Corner May 2016

Fellow Northern Nevada ASIS members,

Our April meeting saw our first Resiliency 2016, conceived and emceed by our own, very talented Kevin Schaller. I thought the event went off very well, and provided a good deal of information to the attendees. As with any event, there are stresses and worries a plenty, but Kevin, John Puccioni, and Darrell Clifton worked their magic to make things come together very smoothly. I wish to convey my deep gratitude to Darrell Clifton and the Circus Circus for hosting the event and comping a good portion of the catering and A/V to make this event very affordable for the chapter. Darrell and the Circus Circus have always been staunch supporters of ASIS and are always willing to chip in to strengthen the organization. It is much appreciated.

I want to remind everyone that we are still soliciting nominations for our 2016 Security Officer of the year, Security Professional of the Year, and the Outstanding Security Achievement or Valor Awards. The deadline has been extended through May 15th. I encourage each of you to consider your colleagues and staff members for these awards and submit nominations to Al Zajic at alanwzajic@aol.com. The awards are an excellent way to recognize folks in your organization for outstanding service. Take the couple minutes required to complete the nomination forms previously sent via email. If you need another form emailed to you, please reach out.

Thank you again for your involvement and participation in the local ASIS Chapter. I hope to see you at the next meeting which will be held at the Washoe County Regional Emergency Operations Center located at 5195 Spectrum Blvd. We will have a chance to see the REOC and will be hearing about the emergency management apparatus in place in Washoe County. It promises to be a pretty interesting meeting.

Inside this issue

Interesting Insider Threat Statistics

When members of our team give presentations, conduct assessments, or teach courses, one of the most common questions is, "Just how bad is the insider threat?" According to the 2010 CyberSecurity Watch Survey, sponsored by CSO Magazine, the United States Secret Service (USSS), CERT, and Deloitte, the mean monetary value of losses due to cyber crime was $394,700 among the organizations that experienced a security event. Note that this figure accounts for all types of security incidents, including both insiders and outsiders. What is especially concerning is that 67% of respondents stated that insider breaches are more costly than outsider breaches.

This dollar figure does not fully account for the damages caused by insiders, though. For instance, activities such as website defacement and exposure of private email correspondence may not involve expensive remediation, but they would still cause a great deal of harm to the victim organization. How valuable is your reputation? How much does your website represent you? If you are an e-commerce company that assures its customers that they will have secure transactions, imagine the damage to your business if your website gets compromised.

Another common question we often receive is, "How many insider attacks take place annually?" This is a much more difficult question to answer. Consider that in the same survey, among 523 respondents, 51% of those who experienced a security incident also experienced an insider attack. The problem with approximating a total number of insider attacks is that, in our experience, a large number of these attacks go unreported. In fact, according to the survey, "the public may not be aware of the number of incidents because almost three-quarters (72%), on average, of the insider incidents are handled internally without legal action or the involvement of law enforcement." There are a variety of reasons why companies choose not to report insider cases; in particular, lack of evidence to prosecute, damage levels that were insufficient to warrant prosecution, inability to identify the perpetrator, and fear of public embarrassment. However, even this does not tell the full story. Based on our research and collaboration with other industry leaders, we believe that most insider

crimes go unreported not because they are handled internally, but because they are never discovered in the first place.

These statistics are rather gloomy for those who defend organizations against insider threat. But the CERT Insider Threat Center has made great progress in identifying patterns of insider crimes, allowing organizations to anticipate and/or detect malicious insider activity before it causes great damage. I have received several stories from attendees in our workshops who have successfully applied recommendations described in our Best Practices Guide to prevent malicious insider activity. So there is hope.

If you have direct experience with insider threat, you can aid our research greatly by sharing your own experiences. Doing so will enrich our data and better inform our methodology, which will in turn be made available to the public in the hopes of improving each organization's defenses. Simply email insider-threat-feedback@cert.org.

https://insights.sei.cmu.edu/insider-threat/2010/10/interesting-insider-threat-statistics.html

Unmasking insider threats

As workplaces become more complex and insider threats become more difficult to detect, a program to mitigate those threats, which include fraud, espionage, workplace violence, information technology (IT) sabotage, intellectual property, and research-and-development theft, can bolster deterrence by providing an early-detection and response mechanism. Moreover, by viewing insider-threat mitigation more broadly than as a cybersecurity challenge, CFOs—working with their CIOs—can help assure the business, protect employees, and safeguard critical data, systems, and facilities.

The goal of insider-threat mitigation is to detect anomalies as early as possible and investigate leads before assets, data, or personnel are compromised. Staying in front of an insider's exploitative tactics, however, requires quick responses, real-time data feeds, and the analysis of behavioral indicators. And in this issue of *CFO Insights*, we'll outline actions to consider when designing, building, and implementing a formal insider-threat mitigation program.

- Define potential insider threats: An insider can be an employee, contractor, or vendor who commits a malicious, complacent, or ignorant act using their trusted and verified access. Still, few organizations have a specific internal working definition, as security and IT budgets have historically prioritized external threats. Defining potential insider threats for the organization is a critical first step to formulating a program, and will inform the size, structure, scope, and phasing plan for the program, aligned to business risk priorities.
- Define the organization's risk appetite: Define the critical assets that must be protected—whether they are facilities, source code, or customer information—and the organization's tolerance for loss or damage in those areas. Identify key threats and vulnerabilities in the business and in the way business is conducted. Tailor the development of the program to address these

http://www2.deloitte.com/us/en/pages/finance/articles/unmasking-insider-threats.html

specific needs and threat types, and take into account the organization's unique culture.

- Leverage a broad set of stakeholders: An insider-threat mitigation program should have one owner but a broad set of invested stakeholders, as well as leadership support. Consider establishing a cross-disciplinary insider-threat working group that can serve as change agents and ensure the proper level of buy-in across departments and stakeholders. The working group should assist in addressing common concerns (for example, privacy and legal) and support the development of messaging to executives, managers, and the broader employee population.
- Take a people-centric approach: The insider-threat challenge is not a purely technical one, but rather a people-centric problem that requires a broad and people-centric solution. Organizations should avoid the common pitfall of focusing on a technical solution as the silver bullet. An insider-threat mitigation program should include critical business processes, such as segregation of duties for critical functions, technical and nontechnical controls, organizational change-management components, and security training programs.
- Trust but verify: Establish routine and random reviews of privileged functions, which are commonly done to identify insider threats across a broad spectrum of areas in a variety of industries. Organizations should trust their workforce, but balance that trust with verification to avoid the creation of unfettered access and single points of failure. Reviews are particularly essential in areas that are defined as critical.

Look for precursors: Case studies analyzed by Carnegie Mellon University's Computer Emergency Response Team program have shown that insider threats are seldom impulsive acts. Instead, insiders move on a continuum from the idea of committing an insider act to the actual act itself. During this process, the individual often displays observable behaviors that can serve as risk indicators for early detection, such as requesting undue access or violating policies, for instance (see sidebar, "Who is an insider threat?"). According to the Federal Bureau of Investigation's Insider Threat Program, detection of insider threats should use behavioral-based techniques, looking at how people operate on the system and off the network, and then build baselines in order to identify anom-

alies.

- Connect the dots: By correlating precursors or potential risk indicators captured in virtual and non-virtual arenas, organizations can gain insights into micro and macro trends regarding the high-risk behaviors exhibited across the organization. Using an advanced analytics platform that correlates outputs from a variety of tools can be helpful, and the output can, in turn, be used to identify insider-threat leads for investigative purposes. Analytics can also shed new light on processes and policies that are either missing or could be improved upon.

- Stay a step ahead: Insiders' methods, tactics, and attempts to cover their tracks will constantly evolve, which means that the insider-threat program and the precursors that it analyzes should continually evolve as well. A feedback mechanism that includes an analysis of ongoing and historical cases and investigations can help organizations adapt their insider-threat programs to address new threats.

- Set behavioral expectations: Define the behavioral expectations of the workforce through clear and consistently enforced policies that define acceptable behavior and communicate consequences for violating policies. Policy areas might include social media, reporting incidents, and bring-your-own-device, for example.

Provide customized training: One size does not fit all. Customize training based on the physical and network access levels, privilege rights, and job responsibilities. Train the workforce to the specific insider-threat risks, challenges, and responsibilities for each position.

Fisher, Anne. "U.S. Retail Workers Are No. 1...in Employee Theft." Fortune US Retail Workers Are No 1in Employee Theft Comments. N.p., 26 Jan. 2015. Web. 02 Mar. 2016.

American Society of Industrial Security Northern Nevada Chapter #164 Secretaries Report

American Society of Industrial Security
Northern Nevada Chapter #164

Secretaries Report

Meeting Date: April 6, 2016
Location: Circus-Circus Hotel Casino, Mandalay Bay B
Members Present: 24, Guest Present: 5
Call To Order: Meeting called to order by Chairman Mark Crosby at 11:27 AM.
Welcome: Chairman Crosby welcomed members and guest.
Introduction of Members and Guest: Members and guest stood and introduced themselves.
Secretaries Report: Reports was published in the newsletter. A motion was made to accept the Secretaries Report, motion seconded and approved.
Treasurers Report: The Treasurers Report was published in the newsletter. Pay-Pal Account $1,955.61 General Fund $ 11,847.02, Scholarship: $4,372.90. A motion to accept the Treasurers Report was made, seconded and approved.
Committee Reports: There were no committee reports.
Old Business: There was no old business presented.
New Business: Members were asked to think about their nomination for Security Professional and Security Officer of the year awards that are coming up June.
Speaker: The meeting was dedicated to Innovations in Organizational Resilience. It was held in a Ted-Talk Model with 5-speakers who spoke for approximately 6-minutes each. The spears were Mark Crosby, Cyber Related Issues, Mike Gach, Active Shooters, Darrell Clifton, Team Planning, Bryan Foote Disaster Recovery, Kevin Schaller, Organizational Resiliency and How It All Ties Together.

Meeting Adjourned at12: 58 PM
Michael S. Gach
Chapter Secretary

ASIS INTERNATIONAL
Advancing Security Worldwide®

Visit the ASIS Northern Nevada site

http://asisnn.org/index.html

ASIS INTERNATIONAL
Advancing Security Worldwide®

Please be advised Future webinars will be offered and notifications will be sent out regularly.

If you feel you are not receiving these notifications please notify Mark Crosby

ASIS Chapter #164

Washoe County Regional Emergency Operations Center located at 5195 Spectrum Blvd

(subject to change-check reader board)

Date: Wednesday, May 4th, 2016

Time: 11:00 AM – 1:30 PM (approximately)

Cost: $20.00 per person

Next Meeting: UNR InNevation Center 450 Sinclair Street Reno, Nevada 89501 June 1st

If you have any suggestions about the news letter please contact Michael Smith

Chairman:	**Mark Crosby**
Vice Chairman:	**John Puccioni**
Secretary	**Mike Gach**
Treasurer	**Cliff Hufnagle**
Membership Chairperson	**Jason McLean**
Newsletter Editor	**Michael Smith**
Law Enforcement Liaison	**Dean Hill**
Legislative Rep	**Ken Braunstein**
Chapter Webmaster	**John Puccioni**
ASIS Foundation Rep	**Steve Foster**
Scholarship Chairman	**Ken Braunstein**
Chapter Photographer	**Ken Braunstein**
Audit Chair	**Ken Lightfoot**
Certification Rep	**Chris Brockway, CPP**
Young Professionals Liaison	**Steve Foster**

ASIS INTERNATIONAL
Advancing Security Worldwide®