Insider Threat Programs at Universities: A Necessary Reality

Protecting the University's People, Campus, Research, and Intellectual Property Against the Insidious Challenges of Evolving Internal Threats

By Stefan Happ, CFE, CPM, MAFF, Inspector, Threat and Criminal Investigation, University of Texas Police at Houston

Stefan Happ, CFE, CPM, MAFF, Inspector

Insider threats are people whose access to an organization enables conduct that is detrimentaal to the organization's goals and mission. Insider threats are usually categorized in a narrow, information security-focused way, but the problem is much greater. Fraud, waste, abuse, larceny, intellectual property theft, and even threats of harm or violence fall into the true definition of an insider threat and are often closely intertwined (Intelligence and National Security Alliance Insider Threat Task Force, 2013, p. 2).

The Risk

Universities are particularly vulnerable, as their organizational complexities, independence of faculty, institutional culture, and open-learning mission can be a fertile ground for insider threats. Contemporary studies indicate that 70 percent of insider threats are through calculation, not impulse (Catrantzos, 2012, p. 7).

The free exchange of ideas and learning may seem at odds with a robust insider threat program, but when sensitive information is compromised, the fallout from the reputational damage may do far more to stifle innovation than a carefully implemented process to protect the campus. Jason du Preez, CEO of data privacy company Privitar, stated that breaches and the damage wrought by insider threats create "devastating loss of self-determination, loss of trust, discrimination and significant economic loss" (Ashford, 2016). Institutions of higher learning must protect their students, faculty, researchers, staff, donors, and communities by providing safe havens for ideas, learning, and human and societal development. Insider threat programs that include the campus safety agency are a potentially effective mitigation tool.

The federal government mandates insider threat programs for any executive branch agency that deals with classified information (Exec. Order No. 13587, 2011) and for most defense contractors (National Industrial Security Program, 2006). In addition, numerous private sector companies institute robust insider threat programs to protect themselves or exceed regulatory mandates. Threats come from predatory competitors that seek to utilize insiders to steal information, disgruntled employees, and others who are inside or have access to the company's information or facilities.

Implementation

Universities share characteristics with the private sector companies and government agencies that have already embraced insider threat teams. Universities conducting cutting-edge research in technology and medicine are almost certainly targeted by others for their intellectual property. Thomas Jefferson University in Philadelphia, Pennsylvania, learned this in 2012 when three cancer researchers allegedly stole intellectual property and moved to the University of Manchester, Manchester, England (Thomas Jefferson University v. Lisanti et al. 2012). The competition between campuses for research funding and private-sector collaborations are prime breeding grounds for insider threats.

Universities should embrace advanced insider threat detection and mitigation processes and form holistic internal partnerships consisting of empowered, high-level stakeholders that can act rapidly to protect the university from all insider threats. Campus police/public safety's skill set may be utilized to protect and serve far beyond the traditional crime and threat role if they are part of this insider threat team. Potential threats include theft of intellectual property, cyber threats, violence and disruption, criminal activity, and exploitation of administrative gaps. If any of these areas is compromised, the university will suffer extreme damage to its reputation, at minimum.

Threats come from predatory competitors that seek to utilize insiders to steal information, disgruntled employees, and others who are inside or have access to the company's information or facilities.

Continued on page 48

Continued from page 47

Institutions of higher learning have complex structures, in which information related to insider threats may be known to a variety of units, such as Compliance, Human Resources, Campus Police, Information Security, and others. These units usually take independent action appropriate to their role, such as the initiation of a compliance investigation, a police criminal investigation, or an information security ticket. However, the information holders may not always share that information with the other potential stakeholders. This inaction can have negative consequences, including a failure to recognize a potential threat. Reasons for not sharing information vary, but most commonly they are due to the information holders not realizing the potential valuable assistance that other units at the campus may be able to provide.

Developing a formal insider threat program is an important progression for institutions of higher learning as they face the threats of an evolving society. Senior executive leadership should sponsor the creation of an insider threat program, involving the most important components of the university, as well as the recommended inclusion of Information Security, Compliance, Legal, Campus Police or Security, Human Resources, Audit, and Behavioral Intervention Teams. Insider threat programs should be highly visible and part of the overall campus' risk-mitigation strategy. Campus education efforts should be carried out to ensure that community members understand the role of the insider threat team and should be encouraged to report perceived threats.

Insider threat teams are typically formed as highly specialized functional teams led by a dedicated risk manager or other highly placed specialist within one of the components who has an established major role in internal investigations.

Carnegie Mellon University's CERT Insider Threat Center states: "An insider threat program is an organization-wide program with an established vision and defined roles. Participating individuals must receive specialized training and the program must have criteria and thresholds for conducting inquiries, investigative referrals, and prosecution requests. Privacy and confidentiality of inquiries must be protected and the program must have full management support" (Collins, et al., p.17).

Insider threat teams, composed of empowered members of all the major campus departments, can greatly reduce organizational barriers and information silos and help the university protect itself through strong teamwork focused on risk mitigation and threat management. Insider threat teams are typically formed as highly specialized functional teams led by a dedicated risk manager or other highly placed specialist within one of the components who has an established major role in internal investigations. They should report to the highest level at the university: to the office of the president or very close, or to an already established high-level committee or council dedicated to policy and procedural improvements in areas that could expose the university to harm.

When insider threats are detected, components of the university should take their appropriate independent actions, but the team should be consulted early for a review and collaboration. Insider threat teams should not oversee any other unit's established or traditional role related to insider threats but should facilitate joint investigations and make recommendations for procedural or substantive process improvements to prevent future similar threats.

Such teams must also include the behavioral intervention team, with law enforcement integration, already in common use on many campuses. Carnegie Mellon University's studies on insider threat typology found that predispositions of disruptive behavior were strong indicators of an insider threat in other areas as well (Carnegie Mellon University, 2016). Revenge behaviors, often presented to behavioral intervention teams, are a common motivation for saboteurs (Kont et al., 2016, p. 15). If such behavior is tracked and mitigated based only on the threats of workplace disruption and violence, and not as part of a greater picture of related persistent threats, the academic institution loses valuable opportunities to more effectively protect itself from an insidious danger.

Considerations

Examining insider threats brings uncomfortable truths to the surface and may expose gaps in ethics and control mechanisms, which may cause reputational damage. While some initially difficult scenarios may bring candid discussions to every level of the institution, the fact that the university created an effective process to improve its operations, eliminate insider threats, and improve its internal risk posture should bring significant improvements to counterbalance some of the initial negative discoveries. Stakeholders generally react very positively to effective self-policing efforts, particularly by public entities.

The insider threat process also can be interpreted as a punitive, disciplinary practice and even a tool to terminate employees. The key to success is to ensure that the insider threat process is part of an extensive risk-reduction education campaign for the entire organization (Intelligence and National Security Alliance, 2013, p. 6). The formation of an insider threat team within a public institution of higher learning must have sponsorship from the highest level, a commitment to support its role completely, published bylaws, and a dedicated communication and education effort to ensure that the goal of the process is not misunderstood. In addition, the insider threat team must be an active consultant to procedural revisions and policy drafting to ensure that future threats are reduced.

Resources

The CERT Insider Threat Center has a series of step-by-step recommendations to help any organization set up an effective insider threat team (Collins et al., p 11-123). These

Continued on page 49

Continued from page 48

recommendations are readily adaptable for institutions of higher learning, although some may require additional work, such as identifying the most critical assets of the university. In addition, some of the strict monitoring and enforcement recommendations may not find ready acceptance in the higher learning environment, which traditionally does not lend itself to rigidity and appearances of obtrusive enforcement of rules.

There are insider threat frameworks other than Carnegie Mellon's CERT program. The American Society of Industrial Security, ASIS International, publishes national standards on risk assessment that contain numerous recommendations applicable for establishing a robust insider threat program (ASIS International, 2015).

Whatever standards the university adopts to implement the insider threat program, all team members should be trained on the confidentiality requirements, methodology, terminology, workflow processes, and procedural rules to ensure consistent, standard appropriate approaches to managing insider threats. Insider threat teams will focus on the most sensitive and confidential areas within the university, so strict confidentiality rules should be written into the bylaws of the insider threat team. All team members should be university employees, and the university's legal officers should be part of the formative process, as well as the eventual insider threat team. Confidentiality exceptions that may exempt the work product and discussions of the insider threat team from public record disclosure laws must be carefully reviewed to ensure that the team's work remains confidential and internal to the institution.

Proven effective in other sectors, insider threat teams can be an innovative way for a university to address the evolving and complex threats facing campuses in a constantly changing world of multiple dangers and should be considered as a potential tool by senior leadership.

References

Intelligence and National Security Alliance (INSA) Insider Threat Task Force, A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector (2013). Intelligence and National Security Alliance.

Catrantzos, Nick. Managing the Insider Threat: No Dark Corners, (2012). CRC Press, New York, NY

Ashford, W. (2016, February 17). University of Greenwich data breach highlights the dangers of insider threats. Retrieved June 09, 2017, from http://www.computerweekly.com/news/4500273276/University-of-Greenwich-data-breach-highlights-the-dangers-of-insider-threats

Exec. Order 13587, 3 C.F.R page 276 (2011)

National Industrial Security Program: operating manual. (2006). Washington, D.C.: Dept. of Defense. doi:http://dtic.mil/whs/directives/corres/pdf/522022M.pdf

Thomas Jefferson University v. Lisanti et al., case number 120704747, Philadelphia County Court of Common Pleas, 2012.

Markus Kont, Mauno Pihelgas, Jesse Wtjtkowiak, Lorena Trinberg, Anna-Maria Osula. Insider Threat Detection Study. (2016) NATO Cooperative Cyber Defence Centre of Excellence, Tailinn, Estonia

Carnegie Mellon University (2016). Workplace Violence and IT Sabotage: Two Sides Of The Same Coin? Retrieved June 14, 2017, from https://resources.sei.cmu.edu/asset_files/Poster/2016_020_001_484243.pdf

Lawson, M. (2012, July 12). Slade returns to TSU for first time since scandal. Retrieved June 09, 2017, from http://abc13.com/archive/8734175/

Matthew L. Collins, Michael C. Theis, Randall F. Trzeciak, Jeremy R. Strozer, Jason W. Clark, Daniel L. Costa, Tracy Cassidy, Michael J. Albrethsen, Andrew P. Moore. Common Sense Guide to Mitigating Insider Threats, Fifth Edition. (2016). Software Engineering Institute, Carnegie Mellon University.

American Society of Industrial Security (ASIS International), Risk Assessment, (2015). ASIS International and The Risk and Insurance Management Society, Inc.