Guidepost

COMBATING INSIDER THREATS FROM THE INSIDE OUT

In today's business environment, managing risk requires a good understanding of the threats which exist outside our organizations but also those that exist within. So often our focus is on keeping the bad guys out, that we sometimes forget about the risks within our own organizations. Understanding your organization's Insider Threat risk and having some common-sense tools to mitigate it, are the first steps to developing a successful strategy.

According to the 2015 Forrester Global Security Survey, 56% of data breaches happened at the hands of business Insiders. Of these breaches, 26% were malicious and intentional. Additionally, today's Insiders are responsible for approximately 80% of the intellectual property losses in our companies. Data breaches and the loss of intellectual property add up to billions in costly expenses for businesses, not to mention the significant reputational damage which happens when these losses become public.

Even more unfortunate is when Insiders are responsible for some of the most horrific events in our workplaces by way of violence. Recently, a workplace dispute between two attorneys ended sadly during the Southern California law firm's holiday party; claiming the lives of both attorneys. Having a significant workplace violent event at the hands of a once trusted Insider (the shooter was a named partner at the law firm) can dramatically and forever change your organization.

So where do businesses start when there are so many things to consider? First and as usual, it starts at the top.

Leadership's understanding of what really matters to your company is paramount. Organizations are best served if they start early in establishing a credible and sustainable security culture. However, no organization can protect everything the same and you can bankrupt your organization trying. Identify your most critical assets, information and systems and build controls around them to provide extra security. According to reports, in the case of the Southern California law firm, the shooter was recently fired from the firm. He freely walked into his former office building and opened fire.

Second, do your due diligence BEFORE you hire employees and others who will have access to your critical information.

Every company has some vetting process around new hires and important partners but each state has different legal limitations. Know the potential and the extent of vetting you can employ around critical hires with access to your most critical data information. Do not solely depend on automated reports and quick checks. Utilize internal and third-party resources to more fully vet individuals in the most impactful roles and with the most important access.

Third, make sure you have clear and well documented employee expectations as part of a sufficient onboarding and offboarding process.

It is common these days, for employers to ask new hires to sign non-disclosure agreements to protect company information. Employees should know in advance what their obligations are relative to critical information and even personal behavior. A thorough Code of Conduct which is explained and trained to, can prevent unnecessary future investigations based on personal behaviors inconsistent with company policies. As employees leave the company, a robust exit interview and reminder of employee obligations should also be part of any employment transition.

Fourth, utilize role-based access to protect specific information.

Not all your employees need, nor should they have, access to all information. Information not limited to but including that containing Personally Identifiable Information and Customer Information should be walled off from most of your employees. Sensitive and proprietary information such as launch plans, research and development and specific internal deliberations should also require special access. Make sure to have a mechanism in place to update access as employees change or leave positions.

Fifth, address the Insider Threat from a holistic perspective.

The Insider Threat is an organizational threat and cannot be sufficiently addressed within a siloed company component. Different parts of your organization need to be at the table to understand and to address Insider Threats. Utilizing assets within Legal, Human Resources, Physical and Cyber Security, as well as Employee Assistance Programs and others can make an effective team. Having an executive sponsor and accountability to senior leadership of the organization will also add to the program's effectiveness and credibility within the company.

Sixth, Train and Assess.

Understanding the behaviors or indicators which may represent an Insider Threat is critical to an effective program. Training employees and management to identify concerning behaviors and report them appropriately not only reduces the organizational risk of an Insider Threat, but can also build a more proactive and caring workforce. The ability to effectively get in front of potentially worrisome behaviors can often provide employees with appropriate support and further a more positive workplace relationship with the employee.

Finally, have an impartial and respectful reporting and investigations process**, well known across the organization.**

Employees need to trust that if they report concerns about behaviors or actions on the part of a fellow employee, their information will be handled discreetly and if warranted, acted upon. Respect and privacy protections for employees need to be built into any process. It is foundational to any trusted process and needs to specifically ensure the protection of potential whistleblowers.

STEPHANIE DOUGLAS

President, National Security Practice

Stephanie Douglas focuses on sensitive internal and white-collar crime investigations, corporate security programs, intellectual property (IP) protection and investigations, and proactively educating executives about insider threats. She has extensive experience in the management of criminal and national security investigations, domestic and global security operations and policy development and strategy. Ms. Douglas has had a distinguished career in both the private and public sectors. After 23 years, she retired as a Senior Executive from the Federal Bureau of Investigations where she served in a variety of influential roles. She also served as the senior director of corporate security for Pacific Gas & Electric prior to joining Guidepost Solutions.