

CYBERSECURITY: KEEPING IP UNDER LOCK AND KEY

Your organization's valuable intellectual property (IP) — its trade secrets, patents, and customer lists — is more susceptible to cyberattack today than it was yesterday. And it will be even more vulnerable tomorrow. In fact, a recent study by the Ponemon Institute found that the number of successful cyberattacks on companies more than doubled over a two-year period, and the resulting financial impact increased nearly 40 percent.

Technology is changing rapidly, and so are the means by which the perpetrators of cybercrimes carry out their nefarious activities. Increased global connectivity and a greater reliance on third-party organizations also heighten the risk of IP exposure.

This issue of *Tone at the Top* explores how audit committees, management, and internal auditors can work to reduce IP exposures and better protect their organizations from crippling cyberattacks.

Valuable Assets

Intellectual property is a fairly generic term that encompasses most of an organization's important

product- and service-related data, the intangible assets that give a company its edge. A confidential client database is a good example, as are marketing plans, customer transaction information, and beta test results. The list goes on.



There was a time when this type of information would be stored, quite literally, under lock and key. However, today's high-tech business environment requires digital storage, remote accessibility, and quick and easy transferability. Keeping IP safe is increasingly difficult because, as business has moved to the digital space, so have criminals.

"From a threat vector standpoint, your phone is probably your biggest risk," says Jeff Spivey, president of Security Risk Management Inc. and board vice president for ISACA, which sets international IT audit and control standards.

"There is malware out there that allows hackers to use your mobile phone to monitor your email, access your passwords, IP, and even remotely operate your phone camera," says Spivey, who will be speaking on cybersecurity at The IIA's [General Audit Management Conference](#) in March.

Invisible Threat

The first step to boosting cybersecurity is to identify the threat. The four main types are: nuisance hackers, state-sponsored attackers, criminal attackers, and “hacktivists,” who may be pursuing agendas related to the environment or human rights.

Common modes of attack include the introduction of a malicious program such as a Trojan, worm, virus, or spyware; password phishing; and denial-of-service attacks intended to crash websites. The results can be devastating, including financial losses, IP theft, reputational damage, fraud, and legal exposure.

Six Steps to Protect IP

Robert Smallwood, IT security consultant and author of *Safeguarding Critical E-documents*, recommends the following six steps for protecting IP:

1. Identify confidential e-documents (document types and categories).
2. Determine where they are created, who needs access to them, and when.
3. Develop information governance (IG) policies to manage and control access to sensitive documents.
4. Enforce IG policies with electronic document security (EDS) technologies, which may include information rights management, data loss prevention, digital signature technology document analytics, or encryption.
5. Test and audit your IG program.
6. Refine policies and continue to evaluate deploying new cybersecurity and EDS technologies.

Most insidious are the so-called “zero-day” attacks, in which hackers break into a database, copy or modify data, and then leave undetected, says Marc Vael, chief audit executive for Smals, which provides IT infrastructure for Belgium’s social services and health care system. Under such an attack, it can be months or even years before the breach is detected, long after the damage has been done.

Holistic Effort

Keeping IP safe from criminals requires all [three lines of defense](#) — IT management, risk management, and internal audit — to stay current on relevant technology and share knowledge to prevent blindspots and silos. David Brand, managing director in charge of IT Audit at consulting firm Protiviti, warns against putting too much of the responsibility on IT managers. Cybersecurity, he says, should be a top risk management concern and a regular part of internal audit plans.

“There is a tendency for organizations to think of cybersecurity as an IT issue, but it is really up to executive management to tell IT what needs to be protected, where that intellectual property resides, and who should have access to it,” Brand says. “Cybersecurity risk is the same as any other kind of risk. It’s just that the asset is electronic instead of physical. You need a good system of internal controls.”

The audit committee’s responsibilities can include setting expectations and accountability for management and assessing the adequacy of resources, funding, and focus for cybersecurity activities. It’s important that audit committees communicate expectations regarding security and risk mitigation.

The Weakest Link

Not all threats are external. As with any risk mitigation effort, people are the weakest link. Vael recommends regular and ongoing employee training from the bottom to the top of the organization. “The biggest issue is understanding,” Vael says. “Explain to me, in my language, the risks involved, what is expected, and what that implies.”

Board Communications

The data generated by boards of directors is as vulnerable to cyberattack as any of the organization's IP. Indeed, according to the Thomson Reuters 2013 Board Governance Survey, more than 75 percent of organizations utilize unsecure, personal email accounts to distribute board documents, and almost 50 percent do not ensure board communications are encrypted. But 52 percent of organizations now use a board portal to share sensitive board information.

As part of the IT audit, Vael recommends an annual evaluation of the organization's ability to maintain and secure its IT applications, assets, and infrastructure — something he calls “e-skills.”

Finally, as more organizations outsource IT functions or move infrastructure and applications to the cloud, Vael urges directors and executives to hold management accountable for doing due diligence on third-party solution providers to ensure that they comply with the organization's policies, practices, and culture when it comes to IP protection and cybersecurity.

“People tend to focus on the tangible stuff — processes and procedures, organizational structures,” Vael says. “What's missing is the cultural component.”

Internal auditors also should verify that the company updates employee training programs as needed so they include requirements for protecting and securely disposing of confidential material, and ensure that new employees have adequate training that includes careful explanation of the information security policy and code of conduct.

Indeed, it is employees who, unfortunately, represent the weakest link in the cyberprotection chain. Organizations can go a long way toward protecting their cyber-IP by doing everything they can to remove the threat from within.

Questions Boards Should Ask



- Which information assets are most critical, and what is the value at stake in the event of a breach?
- Does the board/audit committee spend enough time working to understand the risks and key controls needed to protect the organization from cyberattack?
- Has an inventory of IP been performed, including where it resides and who has access to it?
- Does the organization devote adequate resources and funding to address cybersecurity?
- Has protection of IP been included in the companywide risk assessment?
- Are there formal procedures to be followed in the event of a breach, and have those procedures been tested?
- What is internal audit's assessment of the organization's ability to secure its IP?

Quick Poll Question

How confident are you that your organization's controls can prevent a significant cybersecurity threat?

Visit www.theiia.org/goto/quickpoll to answer the question and see how others are responding.

About The IIA

The Institute of Internal Auditors Inc. (IIA) is a global professional association with 180,000 members in 190 countries. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator. www.globaliia.org

Complimentary Subscriptions

Visit www.globaliia.org/Tone-at-the-Top or call +1-407-937-1111 to order your complimentary subscription.

Reader Feedback

Send questions/comments to tone@theiia.org.

Content Advisory Council

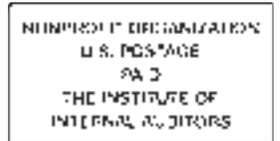
With decades of senior management and corporate board experience, the following esteemed professionals provide direction on this publication's content:

Martin M. Coyne II
Michele J. Hooper

Nancy A. Eckl
Kenton J. Sicchitano



TONE **TOP**
— at the —



247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA

Quick Poll Results

How well do your organization's financial executives, internal auditors, external auditors, and board members communicate with one another?

37%

Poor or Absent



52%

Adequate



11%

Outstanding



*Based on 501 responses. Respondents could only choose a single response.