INTELLECTUAL PROPERTY AT RISK FROM CYBERTHREATS

Trending Topics represents an executive summary compilation of news, information and perspective on matters affecting businesses and business leaders today. This insight is being provided to keep you up to date on the latest developments and trends influencing these topics. These views do not necessarily represent the views and opinions of PNC. For additional research on these topics, please consult the sources cited in this article.

While hacking, identity theft and credit card fraud are in news headlines on a daily basis, very little is written about network breaches that lead to the theft of intellectual property (IP). However, a recent poll by Deloitte found 58% of business respondents expect IP cybertheft to increase in 2017.[1]

Stealing or purchasing stolen IP can be quicker and cheaper than investing in innovation and research, which in turn enables shady organizations to bring new products to market faster. The IP assets most at risk include trade secrets, proprietary business information and copyrighted data such as software codes.[2]

Stolen IP gives cyberthieves and their customers an unfair competitive advantage, and as a result security experts say corporate cyber espionage is on the rise. IP cybertheft is affecting every industry. The sectors expecting the greatest threat increases include utilities and power, telecommunications, industrial products and services, and automotive.[3]

IP theft by an outside attacker often begins through a social media cyberattack such as spear phishing. In this scenario, a cyberthief sends a seemingly innocuous email to an employee with a compromised attachment or link.

While disgruntled current and former employees were once considered the greatest IP theft threat, today's connected digital world enables IP theft to originate anonymously from anywhere. Perpetrators include competitors, suppliers, crime syndicates, recreational hackers and nation states. IP is most often stolen for profit, either for use by a competitor or for sale to the highest bidder.[4]

IP theft by an outside attacker often begins through a social media cyberattack such as spear phishing. In this scenario, a cyberthief sends a seemingly innocuous email to an employee with a compromised attachment or link. When the email is opened, the thief gains entry into the company's network through the employee's email account and can take advantage of system vulnerabilities to access IP and other proprietary company data.

PROTECTING IP FROM CYBERTHEFT

The Deloitte poll noted IP can account for more than 80% of a company's value, yet 44% of respondents believed assessing the value of an IP loss and managing the fallout from a cyberattack would present a major challenge.[5]

Security experts acknowledge that valuing and protecting IP are some of the hardest challenges companies face. Although it may not be possible to completely protect a company's IP, many steps can be taken to significantly reduce the risks of cybertheft. Some recommendations for protecting IP include:[6]

- Identify IP assets throughout the company that need to be protected and update the list regularly, especially after mergers, acquisitions or other major company events.

PNC

Security experts acknowledge that valuing and protecting IP are some of the hardest challenges companies face. Although it may not be possible to completely protect a company's IP, many steps can be taken to significantly reduce the risks of cybertheft.

- Consider conducting a data classification review to assess the sensitivity of data the company holds related to IP and identify what data assets would be valuable to competitors or cyberthieves.
- Establish higher levels of security for the most sensitive data. Often, companies fail to protect IP by relying on the same protocols and controls for valuable IP data that are used for the rest of the company's files.
- Define potential insider threats and establish a threat mitigation program, including access controls, as part of the company's overall network security program and protocols.
- Educate employees continually on cybersecurity protocols, with special emphasis on email and social media attacks.
- Stay current on system and application software patches.
- Keep anti-virus software updated on all systems used by employees, and check systems and devices monthly to ensure compliance.
- Monitor continuously for unusual cyberactivity or events. This can be accomplished with a security information and event management (SIEM) system or other monitoring systems. Maintain logs and review them regularly to spot unusual patterns and alarms that should be investigated promptly.

To discuss these topics in more detail, please contact your PNC Relationship Manager.

1 "Intellectual Property Cyber Theft Expected to Rise," press release from Deloitte on PR Newswire, Oct. 25, 2016.
Available at: http://www.prnewswire.com/news-releases/intellectual-property-cyber-theft-expected-to-rise-300350518.html

2 "The hidden costs of an IP breach," by Emily Mossburg, J. Donald Francher and John Gelinne, *Deloitte Review* and accompanying white paper, issued July 25, 2016.
Available at: https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

3 "Intellectual Property Cyber Theft Expected to Rise," press release from Deloitte on PR Newswire, Oct. 25, 2016.
Available at: http://www.prnewswire.com/news-releases/intellectual-property-cyber-theft-expected-to-rise-300350518.html

4 "The hidden costs of an IP breach,," by Emily Mossburg, J. Donald Francher and John Gelinne, *Deloitte Review* and accompanying white paper, issued July 25, 2016.
Available at: https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

5 "Intellectual Property Cyber Theft Expected to Rise," press release from Deloitte on PR Newswire, Oct. 25, 2016.
Available at: http://www.prnewswire.com/news-releases/intellectual-property-cyber-theft-expected-to-rise-300350518.html

6 "8 ways to protect your company from IP cyber theft," Cash & Treasury Management File, Oct. 28, 2016.
Available at: https://ctmfile.com/story/8-ways-to-protect-your-company-from-ip-cyber-theft;
"French submarine maker data breach highlights challenges of IP security," by Warwick Ashford, *Computer Weekly*, Aug. 25, 2016.
Available at: http://www.computerweekly.com/news/450303120/French-submarine-maker-data-breach-highlights-challenges-of-IP-security

CIB ENT PDF 0117-0148-458902

PNC