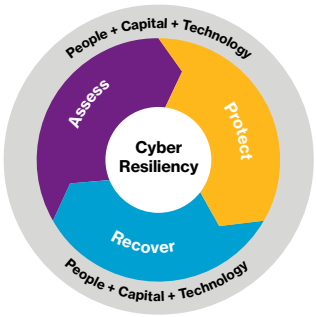


Decode secure.

Emerging cyber risk: Intellectual property theft

by Jason Krauss

In April 2017, a hacking group calling itself "The Dark Overlord" posted 10 unreleased episodes of "Orange is the New Black," even after a $50,000 Bitcoin ransom payment was made. The hackers claimed that the post production studio they hacked violated their agreement by involving the FBI.

A month later, cyber hackers claimed to have stolen a digital copy of *Pirates of the Caribbean: Dead Men Tell No Tales* and threatened to release it in increments online if their exorbitant Bitcoin demands were not met.

And throughout the summer of 2017, a hacker called "Skote Vahshat" stole 1.5 terabytes of data from a leading cable network's servers and attempted to extort $5.5 million worth of Bitcoin. The hacker gradually released stolen materials on the Internet, including unaired episodes of the network's shows as well as script summaries of yet-to-air episodes.

In this case, the hack reportedly was carried out through the purchase of a zero day exploit – one that takes advantage of a software security vulnerability on the same day the vulnerability becomes generally known. In other words, there are literally zero days between the time the vulnerability is discovered and the first attack.

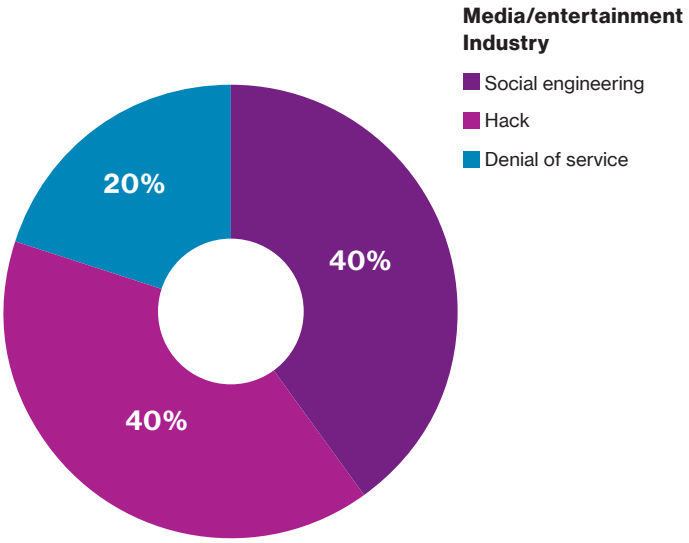
For perspective on how much the risk of intellectual property (IP) theft is growing, consider that the amount of data stolen from the cable network in 2017 was reportedly 7.5 times the amount released by a well-publicized attack on a major media company in 2014. Reportedly, the ransom note indicated that between $400,000 and $500,000 was spent a year to purchase these exploits on the dark web.

Is intellectual property the next cyber target?

While hacks targeting credit card information, consumer health information and other personally identifiable information (PII) still garner the most media attention (primarily due to regulations requiring that PII compromises be reported), IP theft is emerging as another risk weighing heavily on corporate decision makers. Generally defined as creations of the mind, IP can be any type of financial, business, scientific, technical, customer or engineering information that is deemed proprietary. These include inventions, literary and artistic works and symbols, as well as names and images used in commerce.

The incidents against media/entertainment companies described above highlight the emergence of a target for Internet thieves other than banking or other personal information: the IP of an organization or a third party's IP in their care, custody and control.

While hacks accounted for 22% of all incidents in the Willis Towers Watson Reported Claims Index, this number was substantially greater, 40%, within the media/entertainment industry. Historically, the media/entertainment industry has not been a prime target for cyber criminals. But with the industry's explosive growth in recent years, due to the myriad of ways in which we now consume entertainment and the number of outlets that have emerged to meet consumer demand, hackers have recognized the tremendous value in IP as well as the ease by which it can be acquired illicitly.



Understanding the true value of IP

According to Ocean Tomo's 2015 study of intangible asset market value, the value of the S&P 500's intangible assets (of which IP is a subset) grew to an average of 87% by January 1, 2015, an increase of 19 percentage points over 10 years. Further, a report issued by the U.S. Chamber of Commerce states that "publicly traded U.S. companies own an estimated $5 trillion worth of trade secrets." [1]

Many organizations fail to understand the value of their IP and how much of their company's overall value is derived from it. While the two forms of IP most frequently involved in cybercrime are copyrighted materials and trade secrets, cyber thieves will go after whatever is most valuable to an organization in an effort to maximize the extortion potential. For a defense contractor, it could be blueprints for a new weapon system; for a biopharmaceutical firm, confidential data on a life-saving new drug. At a game developer, hackers could obtain the latest new video game, prior to its official release.

Indeed, an organization whose IP is stolen will be faced with a multitude of costs and expenses. Most stand-alone cyberinsurance policies explicitly provide coverage for claims brought by a third-party alleging that IP in the care, custody and control of the victim organization was not properly safeguarded. Coverage could also be available for direct first-party loss, such as:

- Extortion payments
- Forensics costs incurred to investigate the breach and other crisis management expenses
- Public relations expenses
- Data restoration costs

The availability of coverage for other categories of loss associated with the theft, as well as how to establish the less direct, sometimes hidden value of the IP itself, is less clear and would largely depend on the actual claim and damages calculation. One common method of calculating damages in cases alleging theft of trade secrets is "Net Present Value of Future Sales," which is a calculation of the potential revenue of products that would have applied to the trade secret had it not been stolen.

However, that method does not fully contemplate less-quantifiable material damages, such as:

- Loss of product/market advantage to competitors
- Missed business opportunity
- Loss of reputation or brand loyalty
- Declines in stock price or valuation
- Direct loss of profitability

[1] Brian T. Yeh, "Protection of Trade Secrets: Overview of Current Law and Legislations," Congressional Research Service Report (September 5, 2014).

Beyond insurance policies and technological safeguards

IP policies are primarily designed to address financial loss due to legal events impacting the value of an IP right, such as the invalidation of a patent. They may also provide reimbursement for legal costs associated with enforcement of an IP right against third-party competitors. This would include legal costs to pursue a third-party for misappropriating a trade secret or for infringing a patent, trademark, design right or copyright.

For example, in the media incidents described above, a cyber-insurance policy could be implicated if hackers watched stolen episodes and/or sold copies of the creative work to others, thus using the copyright on the creative work without the copyright owner's permission. Therefore, while IP policies provide a valuable benefit with respect to some of the most high stakes "scorched earth" litigation over companies' IP, such coverage is unlikely to play a large role in indemnifying a company for financial losses resulting from the theft of its IP.

Insurance solutions are not always available and technological defenses are never foolproof. As such, organizations must be vigilant in developing a holistic approach to protecting their IP. Such a strategy should include employee training designed to create a culture committed to safeguarding company IP and other confidential information.

Anyone handling sensitive or proprietary data should be trained to identify both outsider and insider threats, including disgruntled workers, careless contractors and negligent suppliers. They must be made to understand the importance of enforcing company standards, policies and procedures aimed at reducing these threats.

Finally, the ability to detect and predict employee behaviors that create vulnerabilities should be increasingly part of an organization's overall cyber risk management strategy. It's practically business-as-usual for any organization interested in protecting and maintaining its competitive advantage in today's threatening environment.

Contact

Jason Krauss
Willis Towers Watson
212 915 8374
jason.krauss@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson