CTRL
Coalition of Technology Resources for Lawyers

The New Information Governance Playbook for Addressing Digital Age Threats

The demand within organizations to manage the growth of electronic information has never been greater. Organizations across the spectrum of industry verticals are generally struggling to address the onslaught of data they both generate and receive. While there is nothing new to this trend, companies should be concerned about new threats arising from that data. From lax internal protocols and unsecured corporate networks to malicious insiders and cyber criminals, these threats—if left unchecked—could threaten the viability of the enterprise.

While some of these factors have posed challenges for years, they are particularly troubling at this time. Cyberattacks are on the rise. The Internet of Things, with its potential to generate revenue, continues to proliferate; as it does so, cybersecurity risks multiply exponentially. Threats are also originating internally as employees increasingly use consumer-grade cloud applications to engage in corporate espionage.

Given the reality of these threats and others, organizations must take proactive steps to govern their information and prepare accordingly. While there is much that could be done to shore up electronic vulnerabilities, the best way to do so is through a holistic information governance strategy. Different from litigation readiness programs of yesteryear that were primarily concerned with preparing for electronic discovery, organizations today need a new information governance playbook that deploys actionable procedures to prevent or mitigate harm from contemporaneous threats to valuable corporate data.

For those organizations that are seeking understanding and guidance on these issues, the Coalition of Technology Resources for Lawyers (CTRL) has prepared this information governance playbook. Developed so companies can better recognize and address the growing risks associated with digital age threats, the playbook should enable them to:

- Learn how cyberattacks, the Internet of Things, and personal cloud use can endanger unsuspecting organizations;
- Develop actionable policies and enforcement mechanisms to protect against risks and strengthen vulnerabilities;
- Craft response plans and communication protocols that mitigate damages; and
- Understand the role that analytics can play in detecting cyber risks and enforcing internal protocols.

I. The Ubiquity of Cyberattacks in the Digital Age

The exponential growth of digital data has brought a corresponding increase in cyberattacks. Notorious incidents involving the Mossack Fonseca law firm in Panama,[1] Ashley Madison,[2] and Sony Pictures[3] have certainly grabbed the headlines.[4] Nevertheless, companies from various industries grapple daily with cyberattacks.[5]

---

[1] Nick Cumming-Bruce & Eric Lipton, *Employee of Panama Papers Law Firm, Mossack Fonseca, Is Arrested in Switzerland*, THE NEW YORK TIMES (June 15, 2016), http://www.nytimes.com/2016/06/16/world/europe/employee-of-panama-papers-law-firm-mossack-fonseca-is-arrested-in-switzerland.html?_r=0.

[2] Claire Reilly, *You blew it, Ashley Madison: Dating site slammed for security "shortcomings"*, CNET (Aug. 23, 2016, 6:47 PM), https://www.cnet.com/news/canada-australia-privacy-report-ashley-madison-avid-life-media-hack/.

[3] Philip Favro, *The Sony Hack Signals The Need For Information Governance*, INSIDE COUNSEL (Jan. 22, 2015), *available at* http://www.insidecounsel.com/2015/01/22/the-sony-hack-signals-the-need-for-information-gov.

[4] According to the non-profit Identity Theft Resource Center (ITRC), there have been 657 data breaches in the United States, exposing 28.6 million records thus far in 2016. If data breaches for 2016 continue at the current pace, 2016 will have the highest number of data breaches since ITRC started tracking in 2005. In 2014, ITRC reported 781 total U.S. data breaches in 2015 and 783 in 2014. *See* IDENTITY THEFT RESOURCE CENTER, 2016 BREACH LIST (2016), *available at* http://www.idtheftcenter.org/images/breach/ITRCBreachReport2016.pdf (includes reported data breaches in the United States from Jan. 1, 2016 through Sept. 8, 2015).

[5] The general business sector accounted for about 40 percent of the data breaches last year. The health/medical sector was second with 35.5 percent, the banking/credit/financial sector accounted for 9.1 percent, government/military was fourth with 8.1 percent, and education was fifth with 7.4 percent of the data breaches in the United States in 2015. *See* IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT RESOURCE CENTER

Whether great or small, one of the principal issues arising from cyberattacks is the resulting expense to the organization associated with addressing breached data. A recent study on the cost of data breaches found the average total cost of those breaches was between $3.79 and $4 million.[6] Viewed from the micro-level, the average cost of each stolen record reflecting sensitive information stands at $158, a 29 percent increase since 2013.[7] Those costs are felt acutely in highly regulated industries where the cost per breached record is substantially higher.[8]

An additional, complicating cost factor for organizations includes legal actions. From consumer civil lawsuits and class actions to regulatory enforcement proceedings, businesses often face staggering costs to remediate the harm flowing from breached data.

For example, Yahoo! Inc. announced in September 2016 that it sustained a data breach two years earlier, which resulted in over 500 million records being compromised. Within hours of the announcement, multiple lawsuits were filed, including a putative class action in California accusing Yahoo! of negligence both in allowing the data breach and in taking almost two years to detect it.[9] No doubt investigations will be initiated by government regulators; all of which could result in tens of millions of dollars in legal fees.[10] This does not include the costs to refurbish brand damage among consumers, a difficult task at best.

Gateways to Cyberattacks

With the massive costs that cyberattacks have levied on organizations, it is worth examining some of the corporate vulnerabilities that have led to those attacks. For while cyber incidents originate from hackers and malicious insiders, weak corporate information governance programs are often the gateway to those attacks. Indeed, most organizations are not prepared to address cyber threats with the policies, training, or technology needed to protect their corporate networks. A recent legal industry report confirmed as much when it found that:

- Only slightly over half of the surveyed enterprises had established protocols "to govern identity and access management;"
- Fewer than 20 percent of the respondents had developed a data map; and
- Less than 20 percent of surveyed companies had cybersecurity insurance to fully cover damages resulting from a data breach.[11]

Despite being unaddressed, many of the gateways to cyberattacks are well known. Email, social networks, and text messages—ubiquitous on computers, smartphones, and tablets—have dominated the cyber breach headlines over the past few years.[12] However, other technologies are multiplying (though not replacing) traditional points of access for

---

BREACH REPORT HITS NEAR RECORD HIGH IN 2015 (Jan. 25, 2016), *available at* http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html.

[6] PONEMON INSTITUTE LLC, 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS (2016), *available at* https://www-03.ibm.com/security/data-breach/. The June 2016 study surveyed 383 companies across various countries including Australia, Brazil, Canada, France, Germany, India, Italy, Japan, Saudi Arabia, South Africa, the United Arab Emirates, the United States, and the United Kingdom.

[7] *Id.* at 3.

[8] *Id.* at 10 (observing that the costs per record in the healthcare vertical were $355 while the cost figure for the financial services industry was $211).

[9] *See* Schwartz v. Yahoo!, Inc., No. 5:16-cv-05456 (N.D. Cal. Filed Sept. 23, 2016).

[10] Of course, the Yahoo! breach isn't the only one resulting in civil litigation. The breaches at Anthem, LinkedIn, Target, and others have resulted in class action lawsuits and government investigations. *See* In re Anthem Data Breach Litig., 162 F. Supp. 3d 953 (N.D. Cal. 2016); In re LinkedIn User Privacy Litig., 309 F.R.D. 573 (N.D. Cal. 2015); In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014).

[11] *See* BALLARD SPAHR & THE ASSOCIATION OF CORPORATE COUNSEL, STATE OF CYBERSECURITY REPORT (Dec. 9, 2015), *available at* http://www.ballardspahr.com/alertspublications/legalalerts/2015-12-09-acc-ballard-spahr-cybersecurity-report.aspx (surveying approximately 1,000 corporate attorneys from 887 organizations around the world).

[12] *See*, *e.g.*, Paul M. Barrett, *Forget the Gossip, These Are the Lessons of the Sony Hack*, BLOOMBERG (Dec. 16, 2014, 10:54 AM), http://www.bloomberg.com/news/articles/2014-12-16/forget-the-gossip-these-are-the-lessons-of-the-sony-hack-i3rklun7.

cyber criminals and insiders.[13] One innovation gaining increasing prominence is the growth of external messaging and collaboration software. Like social networking applications, external messaging and collaboration tools provide employees with a more interactive communication platform than the less flexible feel of email or corporate messaging applications.[14]

One of the more popular messaging and collaboration tools is Slack. Billed as a "messaging app for teams who are changing the world,"[15] Slack touts its multifaceted functionality of discussion "channels" for larger groups, "direct messaging" for one-on-one exchanges, and "private channels" to communicate sensitive information.[16] Users have flocked to Slack, vaulting the company in three years from start-up status to a financial juggernaut valued at approximately $4 billion.[17]

Despite its popularity, the use of Slack may leave companies vulnerable to security lapses and cyberattacks. This is because Slack—like Asana, HipChat, and other collaboration tools—does not utilize traditional enterprise-grade technology that can be integrated into the corporate network.[18] Thus, while employees can use Slack from their company-issued laptops and smartphones, companies currently have limited ability to incorporate security measures to protect login credentials, user information, or corporate assets from further dissemination or attacks.[19] Hooks into consumer level storage options and open APIs into third party offerings are also among the various concerns troubling corporate security professionals over the use of cloud-based collaboration platforms.[20]

Although external collaboration apps present one set of cyber complexities for information governance efforts, there are other innovations that are equally problematic. The growth of the Internet of Things represents a distinct cyber challenge that only figures to increase in the coming years.

II. The Internet of Things: A Growing Storm on the Horizon

Organizations face a wave of security related threats from the expected growth of the Internet of Things (IoT). The IoT represents a unique category of data security problems that are distinct from other cybersecurity challenges. This is due to a confluence of factors including the nature of the IoT, its profit-making potential, and its growth in the coming years.

The Nature of the IoT

The IoT is different from other cyber problems due to its interconnected and often heterogeneous nature. The essence of the IoT is that it encompasses a network of physical objects. Those objects—commonly referred to as

[13] *See* Eric Basu, *Cybersecurity Lessons Learned From the Ashley Madison Hack*, FORBES (Oct. 26, 2015, 11:55 AM), http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#75166e62ed99.

[14] *See* Ellis Hamburger, *Slack is Killing Email*, THE VERGE (Aug 12, 2014, 11:00 AM), http://www.theverge.com/2014/8/12/5991005/slack-is-killing-email-yes-really.

[15] SLACK, https://slack.com (last visited October 6, 2016).

[16] About Slack, SLACK, https://slack.com/is (last visited October 4, 2016).

[17] *See* Eugene Kim, *Slack just raised another $200 million round, and it's now worth $3.8 billion*, BUSINESS INSIDER (Apr. 1, 2016, 12:08 PM), http://www.businessinsider.com/slack-just-raised-another-200-million-round-and-its-now-worth-38-billion-2016-4.

[18] *See* Haje Jan Kamps, *Clearchat Picks A Heavily-Encrypted Fight With Slack*, TECHCRUNCH (Apr. 5, 2016), https://techcrunch.com/2016/04/05/clearchat-rapelcgrq-zrffntvat-sbe-grnzf/.

[19] *See* Avi Turiel, *Lessons Learned from the Slack & Hipchat Breaches*, CYREN BLOG (July 8, 2015), https://blog.cyren.com/articles/lessons-learned-from-the-slack-hipchat-breaches.html.

[20] *See* Graham Cluley, *Slack Security Practices Could Lead to Hackers Eavesdropping on Corporate Internal Chat Systems*, TRIPWIRE (Apr. 29, 2016), http://www.tripwire.com/state-of-security/featured/slack-security-practices-lead-hackers/.

"things"—are embedded with electronics, software, sensors, and network connectivity. This enables these objects to collect and exchange data.[21]

The IoT ranges in size and stature. It affects objects on a micro-level, including traditional consumer goods such as refrigerators, and ovens, together with home HVAC, outdoor watering, and security systems.[22] It also affects macro-level environments, including "smart city" initiatives such as those defined by the Smart City Application Ecosystem (SCALE).[23] As detailed below, the macro-level issues are of particular importance to enterprise cybersecurity initiatives.

Profit and Growth

IoT functionality is enabling enterprises to derive substantial revenue from these connected devices. Businesses currently generate more than $613 billion of additional profits annually from IoT devices.[24] With profits expected to hit $14.4 trillion within a decade, this market of opportunity is fueling tremendous IoT growth. Indeed, five million new devices were added to IoT networks each day in 2015. By the end of 2016, these networks are projected to total approximately 6.4 billion devices.[25]

This growth is not limited to an insular group of organizations. 29 percent of companies from a broad range of industries have reported that they presently offer some form of connected consumer device. An additional 14 percent of companies have announced plans to implement some form of the IoT in 2016.[26]

Risks and Threats

As organizations increasingly rely on IoT devices, they should become aware of the risks and threats these devices present and develop comprehensive governance and risk mitigation strategies accordingly.[27] An essential, preliminary question in this regard is whether all IoT devices present the same level of risk.

To answer that inquiry, the potential risk of breach must be measured against the sophistication of the device. For example, smart consumer appliances such as toasters, each of which has a unique identification number (UID) and an Internet Protocol (IP) address, might easily be compromised. This is due to their dependence on a combination of plug-and-play connectivity coupled with relatively little security hardening.[28] However, a direct breach of a single consumer-facing device—even in the company break room—would likely present a relatively low risk.[29]

---

[21] INTERNATIONAL TELECOMMUNICATION UNION, INTERNET OF THINGS GLOBAL STANDARD INITIATIVE, *available at* http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

[22] A. Sheth, *Internet of Things to Smart IoT Through Semantic, Cognitive, and Perceptual Computing*, 31 IEEE INTELLIGENT SYSTEMS 108–112 (2016).

[23] J. M. Schleicher et al., *Enabling a Smart City Application Ecosystem: Requirements and Architectural Aspects*, 20 IEEE INTERNET COMPUTING 58–65 (2016).

[24] S. Abdelwahab et al., *Enabling Smart Cloud Services Through Remote Sensing: An Internet of Everything Enabler*, IEEE INTERNET OF THINGS JOURNAL 276–288 (2014).

[25] *See* Gartner, *6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015* (2015), *available at* https://www.gartner.com/newsroom/id/3165317.

[26] Chet Geschickter & Jim Tully, *Survey Analysis: Early Adopters of Internet of Things Poised to Make 2016 the Year of the Customer,* GARTNER (2015), *available at* https://www.gartner.com/doc/3210417/survey-analysis-early-adopters-internet.

[27] Wojciech Cellary & Jarogniew Rykowski, *Challenges of Smart Industries – Privacy And Payment In Visible Versus Unseen Internet*, GOVERNMENT INFORMATION QUARTERLY, *available at* http://www.sciencedirect.com/science/article/pii/S0740624X15300058 (discussing a 2013 survey conducted by ISACA (formerly the Information Systems Audit and Control Association), which found that 92 percent of respondents expressed concerns about the information collected by Internet-connected devices).

[28] Vijayaraghavan Varadharajan & Shruti Bansal, *Data Security and Privacy in the Internet of Things (IoT) Environment*, *in* CONNECTIVITY FRAMEWORKS FOR SMART DEVICES 261–281 (Zaigham Mahmood ed., 2016), *available at* http://link.springer.com/chapter/10.1007/978-3-319-33124-9_11.

In contrast, more sophisticated devices such as smartphones and tablets, which have operating systems or messaging capabilities, present far greater threats to the enterprise.[30] That breaches will likely arise from such devices in the future is borne out by empirical data. For example, one recent study found that approximately 70 percent of IoT devices contained one or more significant vulnerabilities, with a combined total of more than 250 vulnerabilities (an average of 25 flaws per device).[31] In addition, 80 percent of the items analyzed failed to require passwords of sufficient complexity while 70 percent did not encrypt communications to the Internet and local network.[32] Still another 60 percent did not use encryption when downloading software updates.[33]

Even though these issues are significant, there is one IoT risk of staggering importance: securing the macro aggregation of data. With the increasing quantity of connected devices at the enterprise level, there is a significant risk that the immense volume of data being captured and stored from connected devices may be unintentionally exposing essential infrastructure devices within the IoT ecosystem to systemic failures.[34] This is due to the fusion of heterogeneous networks required for data aggregation and analysis.[35] If left unaddressed, a failure or vulnerability introduced within one service provider's products could result in catastrophic failures across multiple organizations or industries.[36] This includes power grids, health care providers, building control systems, and national defense systems.[37]

All of this may have a ring of science fiction, but the risks of an IoT compromise are no longer fanciful. Indeed, the U.S. Department of Justice has formed a threat analysis team to study potential national security challenges posed by connected devices, including terrorist threats or other exploitation by state actors.[38] Moreover, several notable hacks or breaches have already been attributed to flaws within IoT systems, including the following:

- A massive attack on security cameras and digital video recorders that disabled French web hosting provider OVH and U.S. security researcher Brian Krebs by flooding their networks with webpage requests and other data.[39]

---

[29] The typical home now contains nearly 75 electrical outlets. When accounting for both hard-wired devices and items consumers plug in only periodically, a household may have as many as 200 to 300 devices connected to sockets, with an ever increasing number of these devices offering some sort of smart interactivity. *See* SAMUEL GREENGARD, THE INTERNET OF THINGS (2015).

[30] *Id.*

[31] HEWLETT PACKARD, INTERNET OF THINGS RESEARCH STUDY (2015), *available at* https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[32] *Id*.

[33] *Id*.

[34] A myriad of devices ranging from "heavy assets" such as aircraft engines to more mundane enterprise systems generate massive amounts of data that can later be utilized in the form of aggregated analytics designed to improve performance over time; however, these data sources could be compromised, resulting in massive service or application outages. A. Sheth, *Internet of Things to Smart IoT Through Semantic, Cognitive, and Perceptual Computing*, 31 IEEE INTELLIGENT SYSTEMS 108–112 (2016).

[35] Shancang Li, Theo Tryfonas & Honglei Li, *The Internet Of Things: A Security Point Of View*, 26 INTERNET RESEARCH 337–359 (2016).

[36] Daeil Kwon et al., *IoT-Based Prognostics and Systems Health Management for Industrial Applications*, 4 IEEE ACCESS 3659–3670 (2016).

[37] C. Basu et al., *Sensor-Based Predictive Modeling for Smart Lighting in Grid-Integrated Buildings,* 14 IEEE SENSORS JOURNAL 4216–4229 (2014).

[38] Dustin Volz, *Justice Dept. Group Studying National Security Threats Of Internet-Linked Devices*, REUTERS (Sept. 9, 2016), http://www.reuters.com/article/us-usa-cyber-justice-idUSKCN11F2FP.

[39] Drew Fitzgerald, *Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks*, WALL STREET JOURNAL (Sept. 30, 2016, 3:11 PM), http://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428. Hackers also leveraged hijacked internet-connected things such as cameras, lightbulbs, and thermostats to attack a top security blogger, who was forced to cancel his account after the attack overwhelmed the blogger's resources. *See* Tim Greene, *Largest DDoS attack ever delivered by botnet of hijacked IoT devices,* NETWORK WORLD (Sept. 23, 2016, 10:53 AM), http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html.

- Malware was recently found on the transit network for the city of San Antonio, Texas. This transpired despite proactive efforts to implement enterprise-grade security on the network.[40]
- An attack on Iranian nuclear facilities was the result of state-sponsored malware known as Stuxnet, which was designed to take-over control systems and meltdown critical centrifuge equipment.[41]
- A vulnerability within Chrysler Jeep's engine control and vehicle braking systems was shown to be accessible using an external cellular connection.[42]

In summary, the risks and threats arising from the IoT are no longer theoretical in nature. Now is the time for organizations to begin taking proactive steps to address these issues.

III. The Rising Threat from Personal Cloud Applications

Consumer-grade cloud applications represent a special case among digital age threats.[43] While personal clouds like Dropbox and Google Drive pose cyber-related risks, their problems are more far-reaching. From information security and litigation readiness to information retention and eDiscovery, personal cloud use among employees implicates a range of troubles for organizations.[44] The threats from personal cloud use to corporate trade secrets are particularly acute given the inherent aspects that make this technology so attractive: cheap and unlimited storage, simplified transfers, and increased collaboration.[45]

Despite these problems, organizations have yet to address the proliferation of shadow cloud use among their employees.[46] Equally troubling, some organizations have implemented "bring your own cloud" (BYOC) policies that officially sanction the use of personal clouds in the workplace without sufficient oversight.[47] Unless addressed through an effective information governance program, either scenario could prove disastrous for the enterprise.

Shadow Use of Personal Clouds

Whether done in violation or in the absence of an express company policy, there should be little doubt that employees are using personal clouds in the workplace.[48] While some employees do so in good faith to facilitate their work, others use clouds clandestinely to sabotage the organization or to help a current employer gain a competitive advantage over their former company.[49] Various decisions exemplify the problems with "shadow" or stealth use of personal clouds across the range of corporate employees.

---

[40] Fabio Bisogni, *Proving Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution?* 43 TPRC (2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2584655.

[41] P. W. Singer, *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons*, 47 CASE W. RES. J. INT'L L. 79 (2015).

[42] Maurice Schellekens, *Car Hacking: Navigating The Regulatory Landscape*, 32 COMPUTER L. & SEC. R. 307–315 (2016).

[43] *See* Frisco Medical Center, L.L.P. v. Bledsoe, 147 F.Supp.3d 646, 652-654 (E.D. Tex. 2015) (discussing defendants' extensive use of Dropbox to remove vast amounts of proprietary information belonging to plaintiff).

[44] Susan Miller, *New Risk On The Block: Bring Your Own Cloud*, GCN (May 23, 2013), https://gcn.com/articles/2013/05/23/new-risk-bring-your-own-cloud.aspx.

[45] Robert L. Mitchell, *IT's New Concern: The Personal Cloud*, COMPUTERWORLD (May 20, 2013, 7:00 AM), http://www.computerworld.com/article/2497860/consumerization/it-s-new-concern--the-personal-cloud.html.

[46] *See* discussion *infra* Part IV.

[47] *See* Andrew Froehlich, *The Buck Stops At BYOC*, INFORMATIONWEEK (Jan. 29, 2014, 12:00 PM), http://www.networkcomputing.com/infrastructure/buck-stops-byoc/870595087 ("BYOC presents a nightmare scenario because data can be copied, duplicated, and ultimately lost or stolen via the various cloud services.").

[48] *See* Danny Palmer, *Cios Worried Cloud Computing And Shadow IT Creating Security Risks*, COMPUTING (July 27, 2015), http://www.computing.co.uk/ctg/news/2419409/cios-worried-cloud-computing-and-shadow-it-creating-security-risks; *See* Thoran Rodrigues, *Cloud Computing And The Dangers Of Shadow IT*, TECHREPUBLIC (Aug. 16, 2013, 12:48 PM), http://www.techrepublic.com/blog/the-enterprise-cloud/cloud-computing-and-the-dangers-of-shadow-it/.

For example, in *Toyota Industrial v. Land*, a managerial level employee (Land) used his Google Drive account to remove hundreds of critical documents from his employer (Toyota) before going to work for a competitor.[50] On the eve of his departure from Toyota, Land placed approximately 800 "files and folders" on Google Drive that included technical specifications reflecting the proprietary design of certain industrial equipment, along with related pricing and financial information.[51] That Land removed and then retained Toyota's proprietary information after his departure from the company—in violation of his non-disclosure agreement—resulted in a court injunction that prevented Land from working for Toyota's competitor.[52]

A similarly instructive case is *RLI Insurance v. Banks*.[53] In *RLI*, the employee (Banks) used a Norwegian cloud provider (Jottacloud)[54] to upload "757 customer claim files and other files containing proprietary information" belonging to her employer (RLI).[55] Banks initially tried to obtain the files through Dropbox, but she was denied access by a web filtering software that blocked Dropbox and other commonly used applications.[56] Undeterred, Banks researched "Dropbox alternatives" that could evade RLI's filtering protocol, opened a Jottacloud account, and used that service to remove proprietary RLI data in violation of her employment agreement.[57] RLI eventually discovered Banks' malfeasance, but only after offering her a severance package subsequent to her dismissal from the company.[58]

Company executives are also guilty of using personal clouds for nefarious purposes.[59] In *Frisco Medical Center v. Bledsoe*, the chief operating officer (Bledsoe) for a Texas hospital (Frisco) used Dropbox to take several classes of proprietary and patient information before leaving Frisco for a new position elsewhere. [60] Frisco did not suspect that Bledsoe had furtively removed proprietary information in violation of her employment agreements until she revealed in an exit interview that "she knew where too many bodies were buried."[61] It was only then that Frisco began investigating Bledsoe's computer usage, discovered the use of Dropbox, and determined the extent of the information she had taken from the hospital.[62]

---

[49] *See*, *e.g.*, Frisco Medical Center, L.L.P. v. Bledsoe, 147 F.Supp.3d 646 (E.D. Tex. 2015); Toyota Indus. Equipment Mfg., Inc. v. Land, No. 1:14–cv–1049–JMS–TAB, 2014 WL 3670133 (S.D. Ind. July 21, 2014).

[50] *Toyota Indus.*, at *3-4.

[51] *Id*. at *4.

[52] *Id*. at *7-8.

[53] RLI Ins. Co. v. Banks, 1:14–CV–1108–TWT, 2015 WL 400540 (N.D. Ga. Jan. 18, 2015).

[54] *See* JOTTACLOUD, https://www.jottacloud.com/ (last visited October 4, 2016) ("Jottacloud is a cloud storage service for individuals and companies that lets you backup, synchronize, store and share files from all your devices. The uploaded data is protected by one of the worlds [sic] strongest privacy laws, with all your data stored in Norway.").

[55] *RLI,* 2015 WL 400540, at *1.

[56] *Id*.

[57] *Id*.

[58] *See* Verified Complaint For Damages And Emergency Injunctive Relief, RLI Ins. Co. v. Banks, 1:14–CV–1108–TWT, at *15-16 (N.D. Ga. Apr. 15, 2014) ECF No. 1 ("Not aware of Defendant's misappropriation of RLI's Customer Claim Files and Proprietary Information, RLI offered Defendant a severance package upon her termination. Defendant had not yet accepted the offer of a severance package when RLI discovered the misappropriation. Based on Defendant's misconduct, RLI revoked its offer of severance to Defendant by letter to Defendant.").

[59] De Simone v. VSL Pharmaceuticals, Inc., 133 F.Supp.3d 776 (D. Md. 2015) (involving a chief executive officer who used Dropbox to steal corporate records belonging to the company).

[60] Frisco Medical Center, L.L.P. v. Bledsoe, 147 F.Supp.3d 646, 652-654 (E.D. Tex. 2015).

[61] *Id*. at *2.

[62] *Id*. at *2-4.

Corporate Approved BYOC Accounts

In contrast to shadow cloud use, some organizations have established a BYOC environment that welcomes employee use of cloud applications.[63] Whether by policy or by practice, corporate IT departments have approved the use of consumer clouds by expressly enabling their functionality.[64]

Nevertheless, that is often the extent of corporate oversight.[65] Beyond requiring a signature on a perfunctory non-disclosure agreement, little effort is made to prevent employees from transferring confidential information from company servers to a personal cloud.[66] Such corporate inaction can be challenging on multiple levels, particularly when an employee leaves the company with proprietary materials and begins working for a competitor.[67]

Just such a scenario transpired in *Selectica v. Novatus*.[68] A former employee (Holt) offered to share Selectica's customer and pricing information with his new employer (Novatus), which he previously uploaded to Box before leaving Selectica.[69] The Box account was not a stealth cloud drive concealed from Selectica.[70] Instead, Selectica expressly authorized Holt to store that data with Box under a BYOC arrangement:

> While employed by Selectica, [Holt] had a company laptop computer, which, *on Selectica's recommendation*, was configured so that it automatically synced to his personal cloud storage account at Box.com. This meant that when Holt saved a file to the laptop, the system pushed a copy to his Box account.[71]

Despite having enabled the BYOC arrangement with Holt, Selectica apparently neglected to disable the Box account or remove any proprietary materials upon Holt's departure.[72] As a result, Holt had full access to the pricing information when he joined Novatus.[73]

[63] *See*, *e.g.*, Selectica, Inc. v. Novatus, Inc., No. 6:13–cv–1708–Orl–40TBS, 2015 WL 1125051 (M.D. Fla. Mar. 12, 2015).

[64] *See* Louis Columbus, *How Enterprises Are Capitalizing On The Consumerization Of IT*, FORBES (Mar. 24, 2014, 6:43 AM), http://www.forbes.com/sites/louiscolumbus/2014/03/24/how-enterprises-are-capitalizing-on-the-consumerization-of-it/#1af595ef6160 ("79% [of surveyed enterprises] report that file sharing and collaboration tools including Box, Egnyte, Google Apps, Microsoft Office 365, GroupLogic, ShareFile and others are pervasively used today. 49% are with IT approval and 30% are not.").

[65] *See* Froehlich, *supra* note 47.

[66] *See* Frisco Medical Center, L.L.P. v. Bledsoe, 147 F.Supp.3d 646, 650-1 (E.D. Tex. 2015).

[67] *See* Toyota Indus. Equipment Mfg., Ltd. v. Land, No. 1:14-cv-1049-JMS-TAB, 2014 WL 3670133 (S.D. Ind. July 21, 2014) (explaining that defendant uploaded confidential information from his former employer to his Google Drive account before going to work for an industry competitor).

[68] *Selectica*, 2015 WL 1125051, at *1.

[69] *Id*.

[70] *Id*.

[71] *Id*. (emphasis added).

[72] *Id*.

[73] *Id*. Selectica eventually sued Novatus for trade secret misappropriation and brought a separate action against Holt for his alleged role in the matter. *Id*. at *2.

Analysis of Cloud Jurisprudence

The above referenced cases involve corporate theft that likely could have been obviated had the organizations taken safeguards to prevent, detect, or monitor employee cloud use. Most of the enterprises relied on little more than non-disclosure and other employment agreements to protect their proprietary information.[74] While those agreements enabled the employers to obtain court victories against the cloud-wielding tortfeasors, they did nothing to stop perpetrating employees from misappropriating company trade secrets.[75] This could have resulted in the disclosure of sensitive information to industry competitors. [76]

With respect to shadow cloud use, none of the employers appears to have established a process to detect stealth cloud applications.[77] The only employer that apparently took anything close to a preventative step was RLI, which deployed the use of a blocking program to prevent personal cloud use.[78] However, even that step proved inadequate since the employee easily circumvented the software filter.[79]

In the BYOC context, Selectica took no action to protect its interest in the corporate information stored in Holt's Box account. Selectica did not seek the account's login credentials, did not monitor Holt's use of the account, did not disable the account when Holt left the company, nor confirmed that Holt destroyed all company information stored in the account. Any one of these steps—and certainly a combination of them—could have prevented the disclosure of sensitive information to an industry competitor.[80]

All of which amply demonstrates that organizations should take action to reduce the risks from personal clouds, regardless of whether the cloud use is shadow or approved.

IV. Steps to Combatting Threats and Mitigating Harm

Despite the complexities that these threats present now and in the future for organizations, they are not insurmountable difficulties. Enterprises can generally ameliorate these problems through a proactive, common sense approach to information governance. In this Part, we discuss some of the key aspects of a governance program that can help address the challenges from cyberattacks, the IoT, and personal cloud applications.

Manufacturing Advances in Security and Analytics

Organizational cybersecurity plans stand to benefit from manufacturing advances that are incorporating security measures into the design of technology. This is particularly the case with IoT devices. For example, some manufacturers are now replacing direct device access with indirect access architecture.[81] Others are exploring the

---

[74] Frisco Medical Center, L.L.P. v. Bledsoe, 147 F.Supp.3d 646 , 2015 WL 7734108, *1-2 (E.D. Tex. 2015); Selectica, Inc. v. Novatus, Inc., No. 6:13–cv–1708–Orl–40TBS, 2015 WL 1125051 (M.D. Fla. Mar. 12, 2015); Toyota Indus. Equipment Mfg., Inc. v. Land, No. 1:14–cv–1049–JMS–TAB, 2014 WL 3670133, *2-3 (S.D. Ind. July 21, 2014). *But see* RLI Ins. Co. v. Banks, 1:14–CV–1108–TWT, 2015 WL 400540, *1 (N.D. Ga. Jan. 18, 2015).

[75] *See* David S. Levine, *School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 WASH. & LEE L. REV. ONLINE 323, 334-35 (2015) (observing that many companies prefer to litigate rather than protect their trade secrets).

[76] *See* PrimePay, LLC v. Barnes, No. 14–11838, 2015 WL 2405702 (E.D. Mich. May 20, 2015) (refusing to enjoin the operation of a former executive's competing enterprise).

[77] *See also* De Simone v. VSL Pharmaceuticals, Inc., 133 F.Supp.3d 776, 796-7 (D. Md. 2015).

[78] *RLI*, 2015 WL 400540, at *1.

[79] *Id*.

[80] *See also PrimePay*, 2015 WL 2405702 (denying plaintiff's motion for preliminary injunction given, among other things, the circumstances surrounding the creation and use of defendant's approved BYOC account with Dropbox); Tom Nolle, *Bring your own cloud: The movement companies can't and shouldn't stop*, TECHTARGET (Apr. 2014), http://searchcloudapplications.techtarget.com/feature/Bring-your-own-cloud-The-movement-companies-cant-and-shouldnt-stop.

[81] Ernesto Damiani, *Toward Big Data Risk Analysis*, in 2015 IEEE INTERNATIONAL CONFERENCE ON BIG DATA 1905–1909 (2015), *available at* https://dl.acm.org/citation.cfm?id=2878279.

use of master-slave models for IoT deployments, restricting updates on the slave device via a secure, cloud-based master system.[82]

While these innovations are useful, they are exceeded by the functionality that analytics now offer for IoT security. This includes built-in monitoring designed to notify users of any unexpected changes to the instrument's core software or permission levels.[83] Applicable to both enterprise and consumer threats, the technology captures device activity level. When such activity is aggregated with the metadata from other users in an ecosystem, it enables a more thorough examination and real-time patching of connected devices as threats are uncovered.[84]

For example, certain technology can detect suspicious activity, such as an attempt to access a user's internal computer camera. Once identified, the device blocks the inbound traffic and alerts the user through a smartphone app. If the activity is authorized, the user can simply select the "unblock" option to allow the connection.[85]

Beyond these manufacturing advances, the growing concern around IoT security is fueling the expansion of data security companies that focus on monitoring and protecting data through the coupling of analytics and IoT Big Data sets. Unlike more traditional technologies such as anti-virus software, these tools combine analytics and machine learning to identify and neutralize threats in real-time by pinpointing data anomalies within the metadata generated from the known universe of connected devices.[86]

Data Mapping for Digital Age Threats

With the benefit of these manufacturing advances, organizations should begin taking steps to reduce digital age risks. As an initial matter, the enterprise must understand what data it generates, receives, and stores. To that end, organizations should regularly scan for all network-connected devices and clouds, identify what they are, and how they interact with the network and beyond.[87]

As new connections are identified, their functions and capabilities must be documented and, to the extent possible, secured or disabled. Such a step is essential for controlling ingress and egress to proprietary information—precisely the data endangered by personal cloud applications.[88] A current and accurate data map will enable organizations to better accomplish these objectives and reasonably account for proprietary records.[89]

---

[82] Manuel Díaz, Cristian Martín & Bartolomé Rubio, *State-Of-The-Art, Challenges, And Open Issues In The Integration Of Internet Of Things And Cloud Computing*, 67 J. NETWORK & COMPUTER APPLICATIONS 99–117 (2016).

[83] Mauricio Tellez, Samy El-Tawab & Hossain M. Heydari, *Improving The Security Of Wireless Sensor Networks In An Iot Environmental Monitoring System, Systems and Information Engineering Design Symposium (SIEDS)*, 2016 IEEE 72–77 (2016), http://ieeexplore.ieee.org/abstract/document/7489330/.

[84] Sathish Alampalayam Kumar, Tyler Vealey & Harshit Srivastava, *Security in Internet of Things: Challenges, Solutions and Future Directions*, 49TH HAWAII INT'L CONFERENCE ON SYSTEM SCIENCES (HICSS) 5772–5781 (2016), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7427903.

[85] *CUJO - Business-Level Internet Security For Your Smart Home,* SECURITYGEM (Sept. 22, 2015), http://www.securitygem.com/cujo-business-level-internet-security-for-your-smart-home/.

[86] *Id.*

[87] David Wetmore & Scott Clary, *To Map or Not to Map: Strategies for Classifying Sources of ESI*, INFORMATION MANAGEMENT (2009), http://content.arma.org/IMM/SeptOct2009/to_map_or_not_to_map.aspx.

[88] *See* R. Mark Halligan, *Protecting U.S. Trade Secret Assets in the 21st Century*, 6 No. 1 LANDSLIDE 1, 3 (2013) (urging companies to adopt "mapping" approaches to better safeguard trade secrets). *See also* Sterling Miller, *Ten Things: Trade Secrets and Protecting Your Company*, CORPORATE LAW ADVISORY (Apr. 27, 2015), http://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2015/04/27/ten-things-trade-secrets-and-protecting-your-company.aspx ("You need an inventory of all of the company's trade secrets . . . [a]n inventory helps you identify what steps are needed to keep those specific items confidential and protected and be clear with the business what items are not considered trade secrets . . .").

[89] *Id.*

Another critical step in this regard is to ensure that default usernames and passwords are changed immediately and that UPnP services are disabled whenever possible.[90] If administrative functions on any given device are limited, applying an appropriate firewall can add at least a layer of protection.[91] Finally, proactive monitoring can help track system integrity while providing real-time analysis of suspicious activity.[92]

In addition, any plan should include security profiles aimed at determining the following:

- What are the connectivity and access control features built into my devices?
- If infiltrated and compromised, does the device allow access to other systems within the organization?
- Does the device contain built-in security, and if so, how robust?
- Does the device run on an operating system or configuration settings that might be exploited by malware?
- What is the projected lifecycle of the connected product or device?
- Should the organization engage outside consultants for targeted penetration testing and vulnerability assessments of devices, especially IoT devices?[93]

Many organizations may feel overwhelmed by the governance complexity surrounding these threats. Nevertheless, they must be in a position to perform adequate risk and threat evaluations that weigh the assumed benefits of using connected devices against the anticipated costs or potential loss of reputation that might accompany a failure or breach.[94] Formal policies related to IoT technologies should be designed in a way that ensures physical security measures and written policies are actively enforced and updated on a regular basis.[95]

The National Institute of Standards and Technology (NIST) provides some guidance concerning IoT security. In NIST Special Publication 800-64 Revision 2 titled "Security Considerations in the Systems Development Life Cycle," the organization recommends developing what is commonly known as the master Concept of Operations or CONOPs document.[96] Unlike a traditional data map, this flexible governance tool provides IoT stakeholders with a roadmap for installation, integration, and on-going auditing.[97] When used in conjunction with an advanced data map, the two documents provide a comprehensive blueprint to an organization's IoT and cybersecurity systems.

Many organizations will likely recognize confidentiality and integrity as two of the three legs that comprise this security principle known as the CIA triad, a model designed to guide policies for information security within an organization.[98] When drafting the master CONOPs documentation, enterprises must address a unique collection of CIA challenges presented by IoT devices. This includes ensuring that personally identifiable information remains segregated from device transmitters or logical objects that may leak data fragments from devices associated with

---

[90] Chris Russell, *Assessing The Risk Of Transformative Technologies*, 2016 COMPUTER FRAUD & SEC. 15–19 (2016).

[91] *Id*.

[92] Oliver Niggemann et al., *Data-Driven Monitoring Of Cyber-Physical Systems Leveraging On Big Data And The Internet-Of-Things For Diagnosis And Control*, VANDERBILT UNIVERSITY & INSTITUTE FOR SOFTWARE INTEGRATED SYSTEMS (2015), https://pdfs.semanticscholar.org/c846/29921b2836ce812a8959edb37158f83627ec.pdf.

[93] Adnan Masood & Jim Java, S*tatic Analysis For Web Service Security-Tools & Techniques For A Secure Development Life Cycle*, *Technologies for Homeland Security (HST)*, 2015 IEEE INTERNATIONAL SYMPOSIUM 1–6 (2015), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7225337.

[94] *See* Parts I & II *supra*.

[95] Antigone Peyton, *The Connected State of Things: A Lawyer's Survival Guide in an Internet of Things World*, 24 CATH. U. J.L. & TECH. 5 (2016).

[96] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SECURITY CONSIDERATIONS IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (2008).

[97] Tomás Seosamh Harrington & Jagjit Singh Srai, *Designing A "Concept Of Operations" Architecture For Next-Generation Multi-Organisational Service Networks*, AI & SOC 1–13 (2016).

[98] Somayya Madakam & Hema Date, *Security Mechanisms for Connectivity of Smart Devices in the Internet of Things*, CONNECTIVITY FRAMEWORKS FOR SMART DEVICES 23–41 (2016), http://www.springer.com/cda/content/document/cda_downloaddocument/9783319331225-c2.pdf?SGWID=0-0-45-1579370-p179950200.

unique identifiers.[99] While relatively innocuous on its own, the aggregated data could reveal sensitive information when combined, analyzed, and recompiled.[100]

At a minimum, an organization's CONOPs documentation should capture the following:

Confidentiality and Integrity

- How will IoT devices be provisioned?
- Is there a method for addressing data segmentation in place?
- Does the organization have policies in place to address inadvertent data leaks or breaches?
- What cryptographic tools can the organization apply and how will those resources be managed?
- Are backup or hot swappable options available in the event of an outage or breach?[101]

Monitoring, Testing, Reporting, and Compliance

- What mechanisms does the organization have in place for security monitoring?
- What information should the systems mine from IoT logs and how is that information analyzed?
- Is data captured and transmitted subject to compliance requirements?
- Are big data analytics tools available to help streamline security monitoring?[102]

Authentication and Access Control

- Can the system be integrated into existing enterprise authentication systems?
- Are access controls sufficient to protect against unauthorized access or modification?
- Can the organization place role-based access restrictions on IoT devices and transmitters?
- Have security roles been provisioned and defined?
- Can access controls be applied on a per device or per datatype basis?[103]

Incident Response

- Define and assign incident response.
- Mapping of business functions to new IoT systems.
- Identify the potential impact of compromised IoT systems.
- Create a comprehensive disclosure and alert policy.[104]

Documentation, Operations, and Destruction

- Define the need for additional security documentation.

---

[99] Dean, et al., *A Privacy Approach for Crowd-Source Analytics Based on Internet of Things Sensor Data - Proceedings on the International Conference on Artificial Intelligence,* THE WORLD CONGRESS IN COMPUTER SCIENCE, COMPUTER ENGINEERING AND APPLIED COMPUTING (2016).

[100] Jules Polonetsky, Omer Tene & Kelsey Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification,* 56 SANTA CLARA L. REV. 593 (2016).

[101] Chad Heitzenrater, Justin King-Lacroix & Andrew Simpson, *Motivating Security Engineering with Economics: A Utility Function Approach*, 2016 IEEE INT'L CONFERENCE ON SOFTWARE QUALITY, RELIABILITY AND SEC. COMPANION 352–359 (2016), *available at* http://ieeexplore.ieee.org/document/7573769/?reload=true.

[102] D. Arora, K. F. Li & A. Loffler, *Big Data Analytics for Classification of Network Enabled Devices*, 2016 30TH INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS WORKSHOPS 708–713 (2016), *available at* http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F7470660%2F7471113%2F07471285.pdf&authDecision=-203.

[103] Ezedine Barka, Sujith Samuel Mathew & Yacine Atif, *Securing the Web of Things with Role-Based Access Control*, CODES, CRYPTOLOGY, AND INFORMATION SECURITY 14–26 (Said El Hajji et al. eds., 2015), *available at* http://link.springer.com/chapter/10.1007/978-3-319-18681-8_2.

[104] Eric Holm, *The Role of the Refrigerator in Identity Crime?*, CYBER-SECURITY AND DIGITAL FORENSICS 1 (2016).

- Create a system maintenance and management plan.
- Create documentation for tracking the IoT product lifecycle.
- Define additional training or certifications for support teams.
- Formalize decommissioning and destruction protocols for IoT devices.[105]

Developing Retention Policies

With a data map in place, organizations can then proceed to develop protocols that reasonably ensure the protection of corporate data.[106] This should include how information is stored and maintained among various devices in the enterprise or with hosted service providers. This is significant for both cybersecurity and litigation purposes as all relevant data within the enterprise could be discoverable and subject to preservation duties.[107] That reality should justify the development of processes and policies around data retention and deletion. As evidenced by the Sony Hack, this is particularly the case for nonessential, obsolete, or superfluous information, which should be purged after a reasonable period.[108]

Although the implementation of procedures and policies can serve to reduce potential risk, it might in some instances provide a false sense of security. Enforcement through audit or other metrics can help ensure that rules developed around access control, deletion, herding, and encryption are actually practiced in a manner that minimizes loss resulting from malicious or inadvertent breaches.[109] More importantly, active enforcement of information governance policies can help investigators respond more efficiently to attacks, allowing them to quickly close security gaps to prevent secondary attacks.[110] By formally assessing and addressing risks in this fashion, organizations will be better prepared to meet these threats in an increasingly interconnected world.

Use Policies Governing Personal Clouds

Beyond information retention, organizations ought to develop policies that address employee use of personal cloud applications.[111] Those policies should delineate whether personal clouds will be permitted and if so, what constitutes an authorized BYOC account.[112] Irrespective of whether an enterprise chooses to ban the use of personal clouds or to adopt a BYOC environment, the policy should include audit and enforcement mechanisms to gauge observance.[113] At a minimum, those mechanisms ought to include the right to monitor, access, and disable employee

---

[105] Min-Jung Yoo, Clément Grozel & Dimitris Kiritsis, *Closed-Loop Lifecycle Management of Service and Product in the Internet of Things: Semantic Framework for Knowledge Integration,* 16 SENSORS 1053 (2016).

[106] A comprehensive information governance plan would take various factors into consideration. They would likely include the length of pertinent retention periods, the ability to preserve data for legal matters, applicable data protection laws, cybersecurity initiatives, and use policies for smartphones and other mobile devices. *See*, *e.g.*, Philip J. Favro, *Getting Serious: Why Companies Must Adopt Information Governance Measures to Prepare for the Upcoming Changes to the Federal Rules of Civil Procedure*, 20 RICH. J.L. & TECH. 5, 25-35 (2014).

[107] Gail Gottehrer, *"Connected" Discovery: What the Ubiquity of Digital Evidence Means for Lawyers and Litigation*, 22 RICH. J.L. & TECH. 8 (2016).

[108] Favro, *supra* note 3.

[109] *See, e.g.,* SECURITIES AND EXCHANGE COMMISSION, CYBERSECURITY EXAMINATION SWEEP SUMMARY (Feb. 3, 2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf (highlighting that 57 percent of surveyed financial firms conducted the recommended audits to ensure compliance).

[110] Rodrigo Roman, Pablo Najera & Javier Lopez, *Securing the Internet of Things,* 44 IEEE COMPUTER SOC. 51–58 (2011).

[111] *See* Philip Favro, *Protecting Corporate Trade Secrets in the Age of Personal Clouds*, THE RECORDER (July 21, 2016), http://www.therecorder.com/id=1202763302804/Protecting-Corporate-Trade-Secrets-in-the-Age-of-Personal-Clouds?slreturn=20160903132700.

[112] *See* Miller, *supra* note 44.

[113] *See* Sophie Vanhegan, *Legal Guidance: Protecting Company Information In The Cloud-Era*, HRZONE (Apr. 23, 2013), http://www.hrzone.com/perform/business/legal-guidance-protecting-company-information-in-the-cloud-era.

clouds.[114] Related procedures will also be required for those organizations that proscribe BYOC use since employees will likely circumvent such a policy.[115] For example, blocking programs like the one used in *RLI*, while no guarantee, are a practicable first step to preventing some personal cloud use.[116]

In a BYOC ecosystem, policies should describe what company data can or cannot be transferred to the cloud.[117] In addition, organizations should require the disclosure of user login credentials for approved cloud applications to better ensure policy compliance.[118] Upon an employee's termination, approved BYOC accounts should be disabled or the company should verify that corporate data previously maintained in the account has been returned or destroyed.[119]

In like manner, non-BYOC organizations should examine terminated employees' computer activity and corporate devices to detect whether there was illicit use of personal clouds.[120] If a comprehensive sweep is cost prohibitive, organizations should consider conducting a review of those employees who most likely have access to sensitive corporate information.[121] Such a step would likely have obviated much of the litigation that ensued in *Toyota Industrial*, *RSI*, *Frisco Medical*, and *Selectica*.

Assess and Secure Collaboration Tools

As with other cloud-based tools, evaluating and securing third party collaboration and project management tools should be part of any formal governance strategy.[122] When evaluating options, organizations assess security features and vulnerabilities and develop policies around these tools that strike the proper balance between security and accessibility. As with BYOC policies, organizations should specify how such tools are used, expressly determine the classification level of data shared within collaboration tools, and whether retention polices should be applied to the organization's collaboration systems.

Incident Response

A final aspect of the new information governance playbook is the need to design an incident response plan for mitigating harm from digital age threats.[123] Essential for addressing cybersecurity challenges, such a plan should include various steps to understand and respond to an attack or breach.

The first step is to have a crisis communications protocol in place. This should include having a dark website ready to be activated with little notice in the event of a cyber incident.[124] Dark sites are essentially corporate sponsored

---

[114] *See id*. (observing that corporate policies must "allow company monitoring of employees' IT activity and work email accounts . . .").

[115] *See id*. ("Employers may also wish to consider . . . implementing IT measures to prohibit uploading of documents onto web-based applications."); RLI Ins. Co. v. Banks, 1:14–CV–1108–TWT, 2015 WL 400540, *1 (N.D. Ga. Jan. 18, 2015).

[116] *See* Vanhegan, *supra* note 113.

[117] *Id.* (explaining that policies addressing personal cloud usage should "expressly prohibit the removal of company documents and information outside the company's systems").

[118] *See* Esther Schindler, *Protecting Corporate Data…When an Employee Leaves*, DRUVA BLOG (Oct. 13, 2014), http://www.druva.com/blog/protecting-corporate-data-employee-leaves/.

[119] *See* Rachel Holdgrafer, *Fix Insider Threat with Data Loss Prevention*, CLOUD SECURITY ALLIANCE (Dec. 10, 2015), https://blog.cloudsecurityalliance.org/2015/12/10/fix-insider-threat-with-data-loss-prevention/; Froehlich, *supra* note 47 ("Lack of IT management and control will quickly put an end to BYOC, even though it has the potential to provide real benefits.").

[120] *See* Miller, *supra* note 44 ("Departing employees constitute one of your biggest risks for trade-secret theft.").

[121] *Id.*

[122] *See* Matt Grech, *Slack Alternatives: 10 Collaboration Tools That Do What Slack Can't*, GETVOIP (Aug. 29, 2016), https://getvoip.com/blog/2016/08/29/slack-alternatives/.

[123] Stefanie Fogel, Jim Halpert, Tara Swaminatha, & Jennifer Kashatus, *Breach Incident Response: An Emergency Preparedness Guide*, DLA PIPER (2015), *available at* https://www.dlapiper.com/~/media/Files/Insights/Publications/2015/02/Breach%20Incident%20Response.pdf.

websites, pages, or feeds dedicated to providing information on the crisis at hand.[125] They offer a means to inform or educate viewers regarding the nature of the crisis and the organization's response. They also provide a gateway to customers that might otherwise be unavailable following a large breach or related failures.[126] In an era of when a brand crisis can become a Twitter hashtag within minutes, the organization should be prepared to broadcast its own voice on the issues.[127]

Having counsel ready to address cyber fallout is another fundamental aspect of incident response. Whether outside the company or part of its in-house legal team, knowledgeable counsel should be aware of pertinent laws and regulations relating to the issues and assist in the company's remediation efforts.[128] This includes competently interfacing with government investigators while simultaneously protecting corporate interests in litigation.[129] In order to accomplish these objectives, counsel should work jointly with the corporate information security team to understand how the attack happened, what was done in response, and what was lost or exposed.

Any incident response plan should also include a public relations team to interact with the media. This is a particularly important step with the changing nature of journalism. Given the impact of the 24-hour news cycle and social networking applications, organizations should have personnel designated to communicate with a unified voice regarding the issues. One-off disclosures from operations-level employees, together with other unauthorized revelations, should be avoided and met with appropriate disciplinary measures.[130]

Conclusion

Advances in technology march on. To keep cadence with that march, organizations must stay current with digital age threats. While there is no elixir to completely eliminate these threats, enterprises can develop a holistic information governance plan to address the issues. By staying abreast of the issues, assessing known organizational risks, implementing reasonable procedures to defend against commonplace attacks, and preparing breach mitigation strategies, companies should be reasonably prepared to address these threats, both now and in the future.

---

[124] Center for Infectious Disease Research and Policy, *Dark Site Stores Emergency Communications Until Crisis Occurs*, UNIVERSITY OF MINNESOTA (2016), http://www.cidrap.umn.edu/practice/dark-site-stores-emergency-communications-until-crisis-occurs; Stephen Bell, *Dark Websites for Crisis Response,* EMA PUBLIC RELATIONS (2016), http://www.mowerpr.com/reputation-management/our-experience/dark-websites-for-crisis-response/.

[125] *Id.*

[126] Bruce T. Blythe, *Blindsided: A Manager's Guide to Crisis Leadership*, ROTHSTEIN PUBLISHING (2d ed. June 5, 2014).

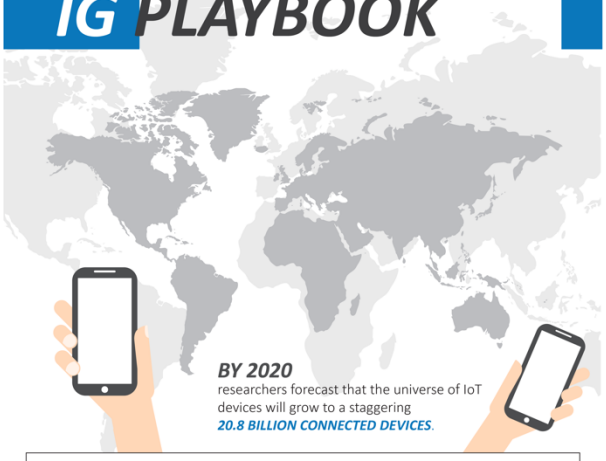
[127] Kim Bhasin, *13 Epic Twitter Fails By Big Brands*, BUSINESS INSIDER (Feb. 6, 2012), http://www.businessinsider.com/13-epic-twitter-fails-by-big-brands-2012-2?op=1/#bitat-abused-trending-topics-to-promote-some-of-its-tweets-9.

[128] *Id.* ("Contact inside and outside counsel to establish a 'privileged' reporting and communication channel.").

[129] *Id.* ("Law enforcement's expertise in evidence gathering and forensics can be leveraged to ensure that the evidence can be used in future court proceedings.").

[130] *See* Toftely v. Qwest Commc's Corp., No. C3-02-1474, 2003 WL 1908022, at *1 (Minn. App. Apr. 22, 2003) (denying plaintiff employment benefits because she was discharged for violating the company's confidentiality policy by disclosing a litigation hold instruction to a third party). In *Toftely*, when a telecommunications company sent a highly confidential and privileged litigation hold instruction to its employees by email, it attached an "electronic tracer" to the message which allowed the company to monitor whether the message was forwarded outside the company. This technique enabled the company to manage the flow of privileged information and ascertain the loyalty of its employees. *Id*.

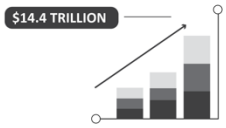
IG PLAYBOOK



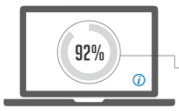
BY 2020
researchers forecast that the universe of IoT devices will grow to a staggering ***20.8 BILLION CONNECTED DEVICES***.

To complicate the issue further, IoT devices are now viewed as a valued source of new revenue for organizations.

According to Cisco Systems, which has established an Internet of Everything (IoE) Index, businesses now generate **$613 billion** of additional profits annually as a result of connected devices.



That number is expected to climb to **$14.4 trillion** in net profits within a decade.



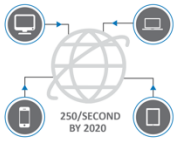
According to a 2013 survey conducted by ISACA (formerly the Information Systems Audit and Control Association), **92 percent** of those ***polled expressed concerns about the information collected by Internet-connected devices.***

Approximately **70%** contained one or more significant vulnerabilities with a combined total of more than ***250 vulnerabilities, or an average of 25 flaws per device.***

Researchers found that **80 percent** of the items analyzed failed to require passwords of sufficient complexity

70 percent did not encrypt communications to the Internet and local network

Another **60 percent** did not use encryption when downloading software updates.



According to Cisco Systems approximately 100 'things' currently connect to the ***Internet every second of every day***; a number that is expected to reach **250 per second by 2020**.

CTRL
Coalition of Technology Resources for Lawyers

SOURCES

- See 6.4 Billion Connected" Things" Will Be in Use in 2016, Up 30 Percent From 2015, Gartner, Inc (2015)
- Wojciech Cellary & Jarogniew Rykowski, Challenges of Smart Industries – Privacy and payment in Visible versus Unseen Internet, Government Information Quarterly
- Hewlett Packard Enterprise, Internet of Things research study, HP IOT RESEARCH STUDY (2015).