Illinois Parks Association Risk Services
"The Choice for Illinois Park & Recreation Districts"

IPARKS UPDATE

A QUARTERLY NEWSLETTER FALL 2016

Be Sure to Update Your Info @ www.iparks.org/Contact Us

Don't Forget!

Routing

(Name)

❑ _____

❑ _____

❑ _____

IAPD
Illinois Association of Park Districts
The IAPD Self-Insurance Program

Cyber Liability for Park Districts

By Chrissie Peterson, Esq., Heyl Royster

Major security and data breaches have become more prevalent in the past decade. News headlines are dominated by stories of major corporations having networks hacked and subjecting employees' and customers' personal, financial and health information to cyber threats. Perhaps one of the following will sound familiar:

- Snapchat had the names and phone numbers of 4.5 million users compromised
- Kickstarter had personal information from 5.6 million donors compromised
- Ebay's database of 145 million customers was compromised
- iCloud had celebrity photostreams hacked
- Sony Pictures had the highest profile hack of 2014 involving email accounts, video games and movie releases.

I. A Real Risk to Local Governments, Including Park Districts

Private entities are not the only ones being attacked by "cybercriminals." On July 14, 2015, the Office of Personnel Management announced that personal data, including social security numbers and fingerprints, for approximately 21.5 million people had been stolen from the U.S. government's databases. While a breach of this size and scope has far-reaching intelligence, financial and political implications, even data breaches for smaller units of government, including park districts, have long-lasting and sometimes irreparable effects.

Consider the headlines:

- On March 10, 2015, a cyber attack on the Town Hall in Orange Park, Florida, took nearly $500,000 from the town's bank account, but the theft was caught in time for a wire transfer to be reversed. Jim Schoettler, *Computer hack at Orange Park Town Hall last month nearly cost $500,000*, The Florida

Cont'd on pg. 2

Cont'd from pg. 1

Times-Union Jacksonville.com (March 10, 2015, 9:21 AM).[1]

- On April 13, 2015, a group demanding the dash camera video of a shooting be released to the public anonymously hacked into the database of the Grapevine Police Department in Grapevine, Texas, and posted a video demanding the release. Dianne Solis, *Anonymous hacker-group demands police video of shooting of Mexican immigrant by Grapevine cop*, The Dallas Morning News-The Scoop Blog (Apr. 13, 2015, 2:34 PM).[2]
- On April 22, 2015, officials with the Wake County Public School System in Raleigh, North Carolina, had to take dozens of school websites offline after a server was hit by hackers. Adam Owens, *Hackers hit Wake public schools server*, WRAL.com (Apr. 22, 2015).[3]

Trends suggest that public bodies will continue to become the targets of data breaches. The smaller the unit of government, the less prepared it is to weather a cyberstorm.

II. What Happens/How It Happens

In 2014 and 2015, Verizon Enterprises published studies indicating that public bodies are among the top three industries where data breaches occur, 2015 Data Breach Investigations Report (DBIR).[4] While data breaches can occur in many ways, and hackers find new methods to access information every day, data breaches at public bodies, including park districts, can generally be classified into one of three categories.

A. Miscellaneous Errors

The most common data breach for public bodies occurs when Miscellaneous Errors happen. These Miscellaneous Errors are described as any mistake that compromises security by posting private data to a public site accidentally, sending information to the wrong recipients or failing to dispose of documents or assets securely. 2015 DBIR, pg. 49.

The Illinois Freedom of Information Act (FOIA) declares that "[i]t is a fundamental obligation of government to operate openly and provide public records as expediently and efficiently as possible…." 5 ILCS 140/1. In other words, local governments, including park districts, are in the business of providing information and, in doing so, unintentional errors occur. For example, consider a request under FOIA asking for all payroll information for all park district employees for the month of January, 2016. In response, the FOIA officer provides a payroll report from the month of January, but accidentally forgets to redact the social security numbers of the employees listed.

B. Insider Misuse

The second most common data breach is classified as Insider Misuse, when employees or those with access to the information misuse it. 2015 DBIR, pg. 46. These are not situations where unintentional errors occur, but an employee or someone with access to the information intentionally accesses the data to use it for an unlawful purpose. For example, a disgruntled accounting clerk accesses patron information to obtain the name, date of birth and bank account information in order to fraudulently establish a credit card in that patron's name. Consider another scenario where a third party vendor, a benefits provider, for example, handles employee information. Once transmitted, the park district loses control over information security for that data. Savvy park districts will make sure their contracts with vendors make the vendor responsible for any data breach that occurs during the engagement and that it will indemnify the park district for any actions arising from such a breach.

C. Theft

Finally, data breaches can result from physical theft or loss of laptops, tablets, smart phones, USB drives or even printed documents. 2015 DBIR, pg. 45. For example, consider a scenario where a Human Resource director is heading to a conference and his/her laptop is stolen. The laptop is not encrypted or passcoded and the thief can access all the employee files the director keeps on his/her computer.

III. Statutory Limits and Protections

At all levels of government, laws have been aimed at narrowing the information that can be collected initially by public bodies and with whom it can be shared, as well as mitigating a breach after it occurs.

In Illinois, the Identity Protection Act is intended to control the collection and use of social security numbers by state and local government agencies. The Act specifically prohibits certain uses of social security numbers at public institutions and agencies, and creates collection and protection requirements. 5 ILCS 179/1 *et. seq.*

The Act recognizes, however, the business necessity of collecting and disclosing social security numbers in certain instances.

Federal regulations like the Health Insurance Portability and Accountability Act (HIPAA) limits the collection and use of protected health information, and also has requirements for entities suffering a data breach, including customer notification and damage mitigation provisions, such as mandatory credit monitoring and fraud protection for affected customers.

The Personal Information Protection Act requires government agencies, corporations, universities, retail stores or other entities that handle nonpublic personal information to notify each Illinois resident who may be affected by a breach of data security. 815 ILCS 530 *et. seq.* Personal information is defined as: an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(1) Social security number

(2) Driver's license number or State identification card number

(3) Account number or credit card or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

815 ILCS 530/5.

The required notice to Illinois residents must include contact information for credit reporting agencies and the Federal Trade Commission, along with a statement that the individual can obtain information from those sources about fraud alerts and security freezes. 815 ILCS 530/10(a). If the data breached is data that the entity owns or licenses, the notice must be made without unreasonable delay. *Id.* If the data breached is data that the entity does not own or license, notice must be made immediately. 815 ILCS 530/10(b).

Failure to notify affected consumers is a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act. 815 ILCS 530/20.

IV. Risk Management

Technology is everywhere. Smart phones, tablets, laptops, the internet, online bill payments and the like have changed the way public entities, including park districts, operate. A concerned citizen no longer needs to go to an administrative office to receive services. Public meetings are often broadcast on the local public access channel. Applications and participation forms can be downloaded and/or submitted online. Monthly fees can be automatically debited from checking accounts.

As you incorporate these practices into your operating structures, there are risk management tools that park districts should be aware of and use on a daily basis. Anti-virus software, passwords on all devices, frequent backup of data, and encryption for sensitive information transmitted electronically are just a few.

What if a park district takes all the steps necessary to reduce the risk of a data breach and it still occurs? There is a way to reduce damages and to shorten the recovery and restoration timeframes.

Cyber Liability insurance can protect public bodies from data breaches that result from malicious hacking or other non-malicious digital risks. This specific line of insurance was designed to insure consumers of technology services or products from liability and property losses that may result when a business engages in various electronic activities, such as selling on the internet or collecting data within its internal electronic network.

Most notably, cyber and privacy policies cover a public body's liability for data breaches in which the constituents' personal information (such as social security or credit card numbers) is exposed or stolen by a hacker. The cost of a data breach can be enormous and we have yet to see a public body budget a line item for "data breaches." Cyber liability insurance is one way to limit or minimize your total financial exposure in that situation.

Just as your organization works to maintain facilities and programming, you must now work to maintain data privacy at all levels of your organization.

IPARKS provides its members with Cyber Liability coverage.

Chrissie Peterson is Of Counsel with Heyl Royster. Chrissie's practice is focused on government law, representing municipalities and other public entities in a broad range of issues, including administrative and regulatory law, the operation and governance of critical services, employment matters, infrastructure construction and financing, council procedures, tax increment financing and economic development.

[1] http://jacksonville.com/news/crime/2015-03-10/story/computer-hack-orange-park-town-hall-last-month-nearly-cost-500000

[2] http://thescoopblog.dallasnews.com/2015/04/anonymous-hacker-group-demands-police-video-of-shooting-of-mexican-immigrant-by-grapevine-cop.html/

[3] http://www.wral.com/hackers-hit-wake-public-schools-server/14599060/

[4] http://www.verizonenterprise.com/DBIR/2015/?&keyword=p6922139254&gclid=CNOK7pmn-cQCFUJrfgod2DcAUQ