Protecting Your Most Important Asset…

Information

Christy Pernitzke

SysLogic, Inc.

About Me

Christy Pernitzke
Director of Delivery Services
SysLogic, Inc

Over 20 years in the technology field, including software development and information management

Experience in Finance, Banking, Healthcare, Manufacturing, and Non-Profit Sector

Help organizations navigate, adapt, and thrive in our new digital world

SysLogic

A Brookfield, Wisconsin based information systems consulting and services firm dedicated to helping clients large and small conduct business more effectively by delivering solutions that leverage leading-edge technology and sound business processes.

Information more valuable than Oil?

Source: The Economist

Corporations and the government leverage mainframes to store and analyze survey data such as census and consumer purchasing habits.

1960's

Netscape is credited with inventing the browser "cookie" allowing firms to build a profile of a user by recognizing and tracking his or her Web surfing behavior.

1994

Facebook is established. Massive amounts of personal information is entered by users. This information is eventually shared with Facebook partners to support targeted marketing.

2004

The iPhone is released ushering in the 'smart phone' era. The introduction of the App Store the following year opens the door for 3rd party mobile applications to collect a wide array of information.

2007/2008

1979

Online shopping is invented when Michael Aldrich connects a modified domestic television via a telephone line to a real-time multi-user transaction processing computer.

1995

Online shopping giants Amazon and eBay are launched. Online payment information, purchasing history, and buying preferences are collected and stored for millions of users.

2006

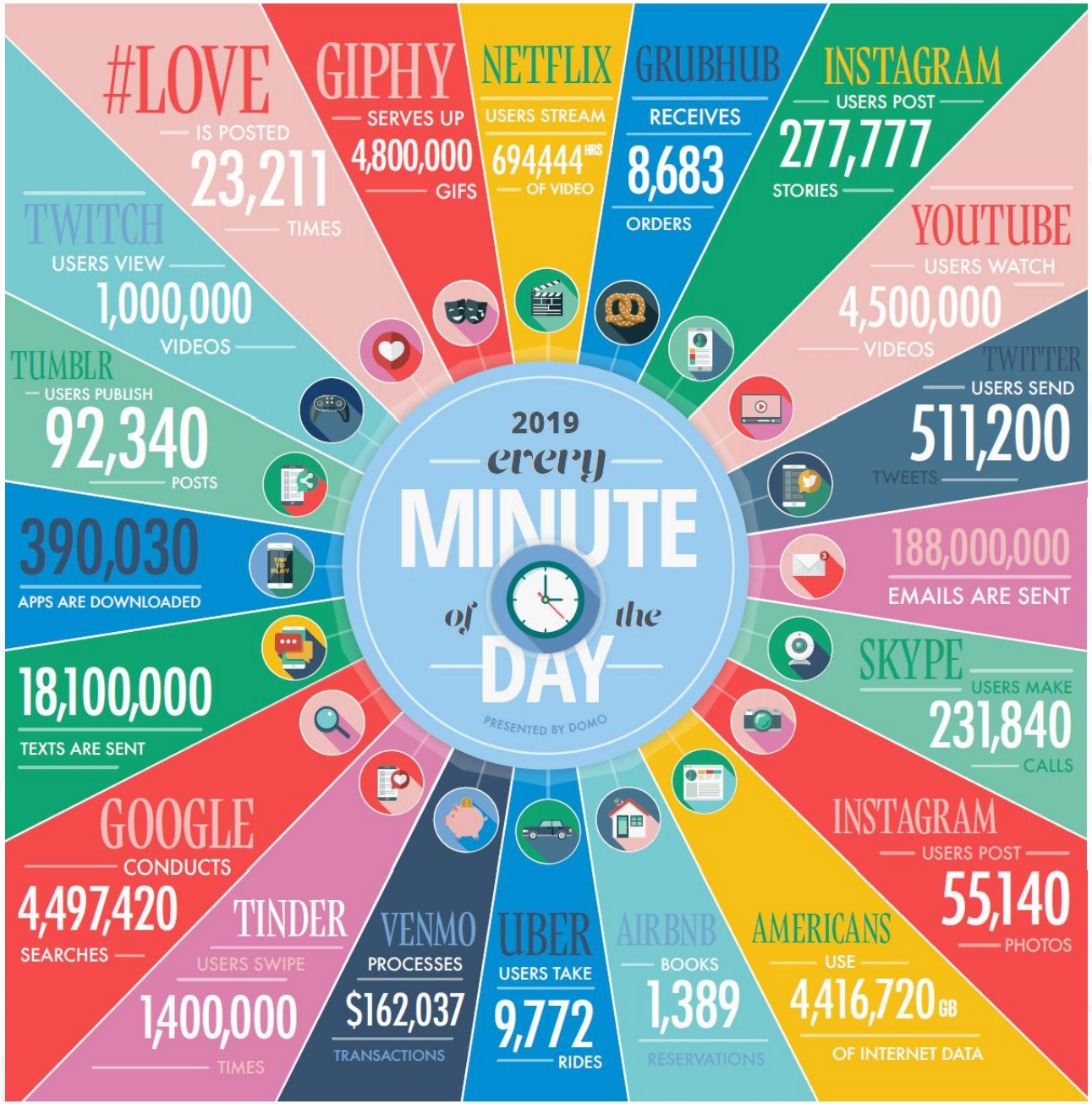
Google Analytics is made available to the public. This platform will greatly shape the way web and mobile data is tracked and analyzed

2013

Amazon releases the Echo which starts the "Smart Home" boom leading to data collection from appliances and much more

Today

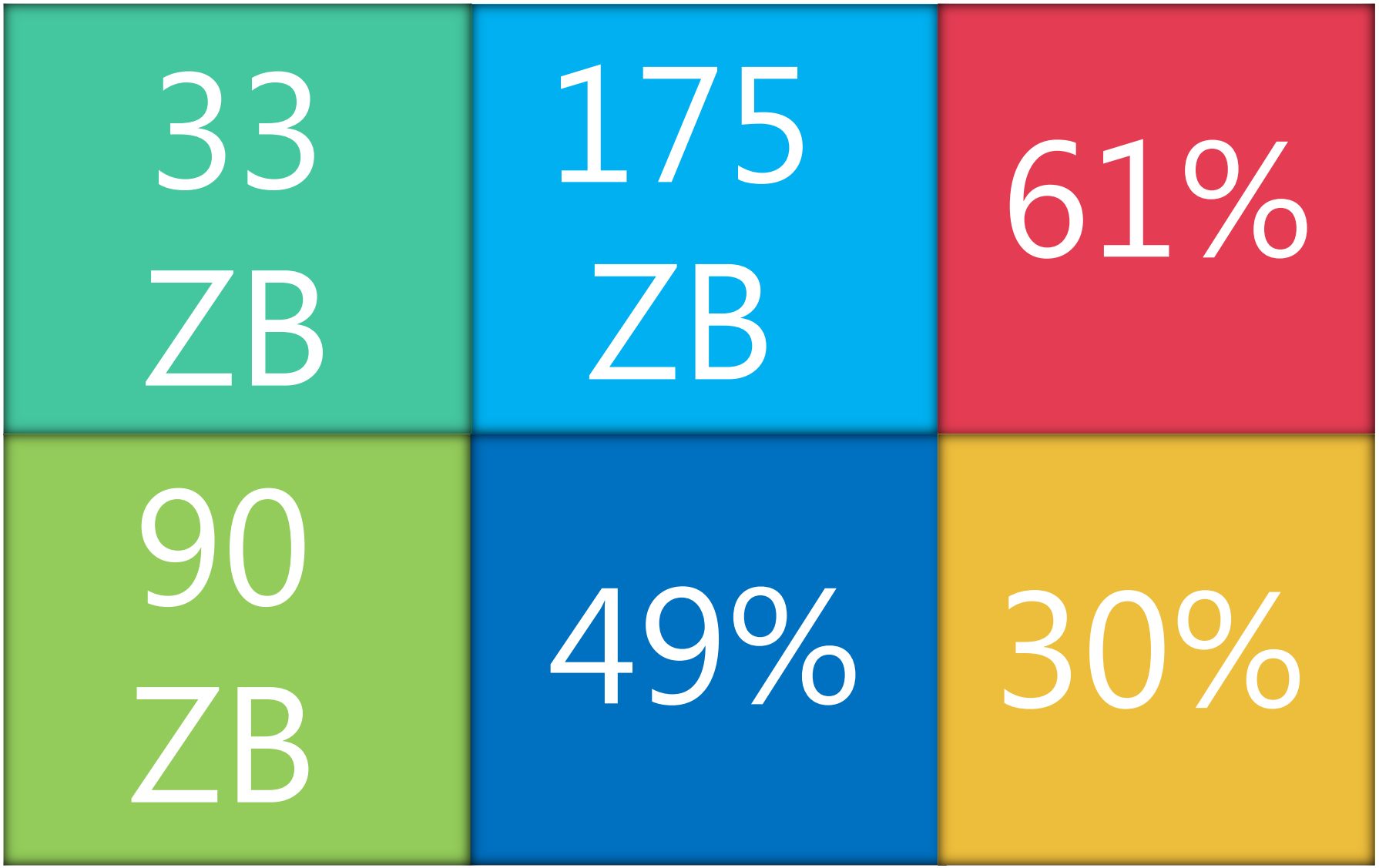
- Online account passwords
  - Fingerprints, retina scans, facial recognition
- Banking and financial information
- GPS tracking of your current location
- Time and location of events you have attended
- Search engine history
- App usage
- Photos
- Social media activity



SOURCES: STATISTA, INTERNET LIVE STATS, EXPANDED RAMBLINGS, NATIONAL ASSOCIATION OF CITY TRANSPORTATION OFFICIALS, WIRED

DOMO

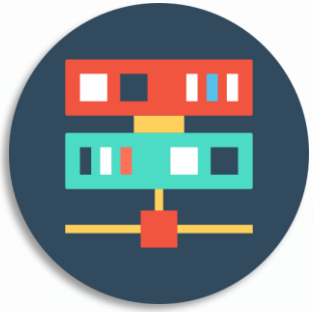
World's Data by 2025



Source: IDC

What are we doing with all that data?

Products
Improve products or look for opportunities to create new products and/or services



Customers
Gauge customer satisfaction, buying patterns, and preferences

Processes
Improve external and internal processes to reduce costs, increase productivity and efficiency, etc.

Nothing
Much of the data being collected isn't being used


BUSINESS
NEWS
DATA STOLEN
DATA BREACH
FINANCIAL NEWS
DATA BREACH
NEWS TODAY
HACKED!

Significant Data Breaches

Equifax

2017 data breach that exposed sensitive information on over 147 million consumers, costing it about **$650 million**

Capital One, March 2019

140k American SSNs and 80K bank account numbers stolen along with tens of millions of credit card applications estimated to cost up to **$150 million**

Zoll Medical Corp, Nov-Dec 2018

280k patient's personal and medical data was compromised after an error was made during a server migration

Verifications IO, March 2019

2 million unencrypted records were leaked containing sensitive information of its users

FEMA, Jan 2019

1.8 million people had both their banking information and addresses were unnecessary shared with a third-party vendor

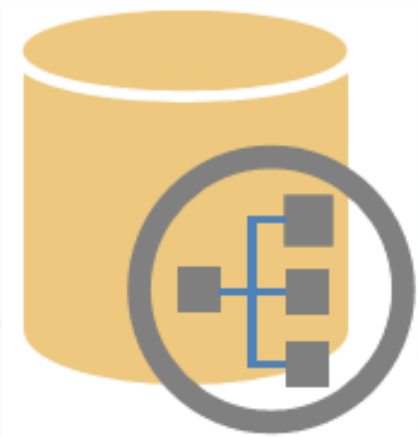
Facebook, April 2019

Hundreds of millions of Facebook users' records were exposed publicly by 3rd party app developers

What to consider

Risk Categories

Technical Architecture and Infrastructure

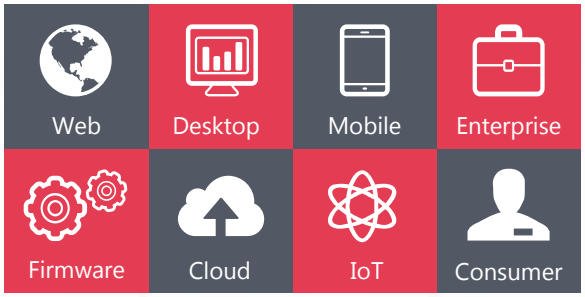


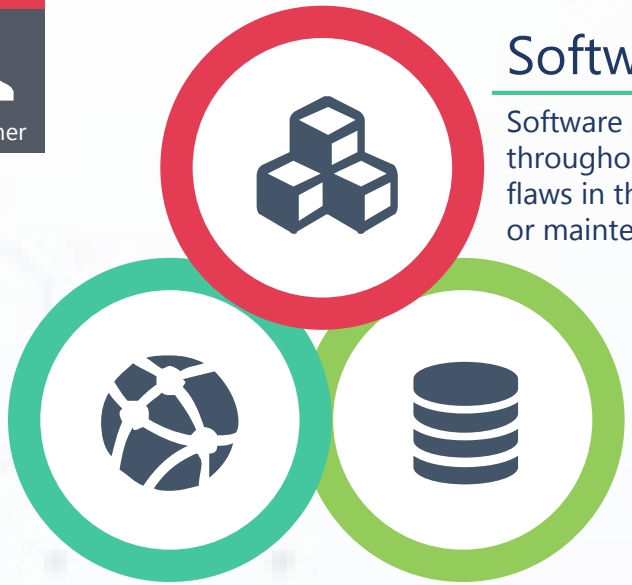
Physical Security

Regulatory Requirements

People

Technical Architecture and Infrastructure





Software Security

Software security encompasses measures taken throughout the code's life-cycle to prevent flaws in the design, development, deployment, or maintenance of the system

Network Security

Network security involves procedures to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and resources

Data Security

Data security involves protecting data stores, such as a database, from malicious and negligent forces, and from the unwanted actions of unauthorized users

Physical Security

- Offices
- Server Rooms
- Laptops
- Smart Phones

The Numbers…

1 in 4 US workers admit to leaving their computer on and unlocked when they go home at the end of the day

Nearly half of C-Suites indicate that they have had employees who lost or had their company laptop/device (49 percent) or company mobile phone (43 percent) stolen

1 in 5 C-Suites (17 percent) and Small Business Owners (18 percent) suffered a data breach due to an employee losing or having sensitive information stolen

Source: Shred-it, June, 2018 Shred-It Study Exposes Employee Negligence as Top Information Security Risk to U.S. Businesses

Regulatory Drivers

Various regulations around the world seek to improve software and data security

US Federal Trade Commission

The FTC settles cases against companies that failed to reasonably protect consumer's personal data.

California Consumer Privacy Act

Grants consumers the right to know what private information is collected, and with whom it is shared it.

HIPAA/HITECH

Defines administrative/physical safeguards and access control requirements for healthcare systems.

General Data Protection Regulation

GDPR: A regulation in EU law on data protection and privacy for all individuals within the European Union.

FERPA

Governs the access to educational information and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments.

Brazil: Resolution No. 4,658

Cybersecurity requirements for financial institutions that are regulated by the Brazilian Central Bank.

People

Social Engineering

Insider Data Theft

Man-In-The-Middle

People

Social Engineering leverages the concept of “trust” on which social networks are built

Phishing

Fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Whaling

Targeted attempt to steal sensitive information from a company such as financial information or personal details about employees, typically for malicious reasons. Size of the targets are larger relative to those of typical phishing attacks.

Watering Hole

Victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group becomes infected.

Pretexting

Focus on creating a good pretext, or a fabricated scenario, the attacker can use to try and steal their victims’ personal information. These types of attacks commonly take the form of a scammer who pretends that they need certain bits of information from their target in order to confirm their identity.

Baiting

Although similar to phishing attacks, what distinguishes baiting from other types of social engineering is the promise of an item or good that hackers use to entice victims. Baiting person may offer users free music or movie downloads, if they surrender their login credentials to a certain site.

Quid Pro Quo

Promises a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good.

A common type of quid pro quo attacks involve attackers who impersonate IT service people and who spam call as many direct numbers that belong to a company as they can find and offer IT assistance to each and every one of their victims.

People

What kind of internal threats are you most concerned about?

71%

Inadvertent data breach/leak

(e.g., careless user causing accidental breach)

68%

Negligent data breach

(e.g., user willfully ignoring policy, but not malicious)

61%

Malicious data breach

(e.g., user willfully causing harm)

https://security.haystax.com/blog/ebook/insider-attacks-industry-survey/

People

A malicious man-in-the-middle attacker can spoof local WiFi access points

Once connected, activity that is shared across WiFi can be monitored including gathering of information like…

- Login credentials
- Intellectual property
- Email

How Do I Protect My Information?

Physical Access/Security

- Granted by an appropriate Data Steward
- Secured to prevent unauthorized access
- Paper or written forms are properly secured
- Procedures formally documented and followed, including logging and monitoring
- Regular review and reauthorization of access by an appropriate Data Steward
- Access is revoked in a timely manner for people who no longer require it

Data Stewardship and Governance

- Overall management of the availability, usability, integrity, and security of data used in an enterprise
- Developing and enforcing guidelines that include what data is necessary for each business function is critical

Security Patches

Software

Business Applications

Database Management Systems

Web Browsers

Operating Systems

Hardware

Laptops

Desktops

Servers

Door Locks

Firmware

Routers

Cameras

Printers/Scanners etc.

Phones

Password Security

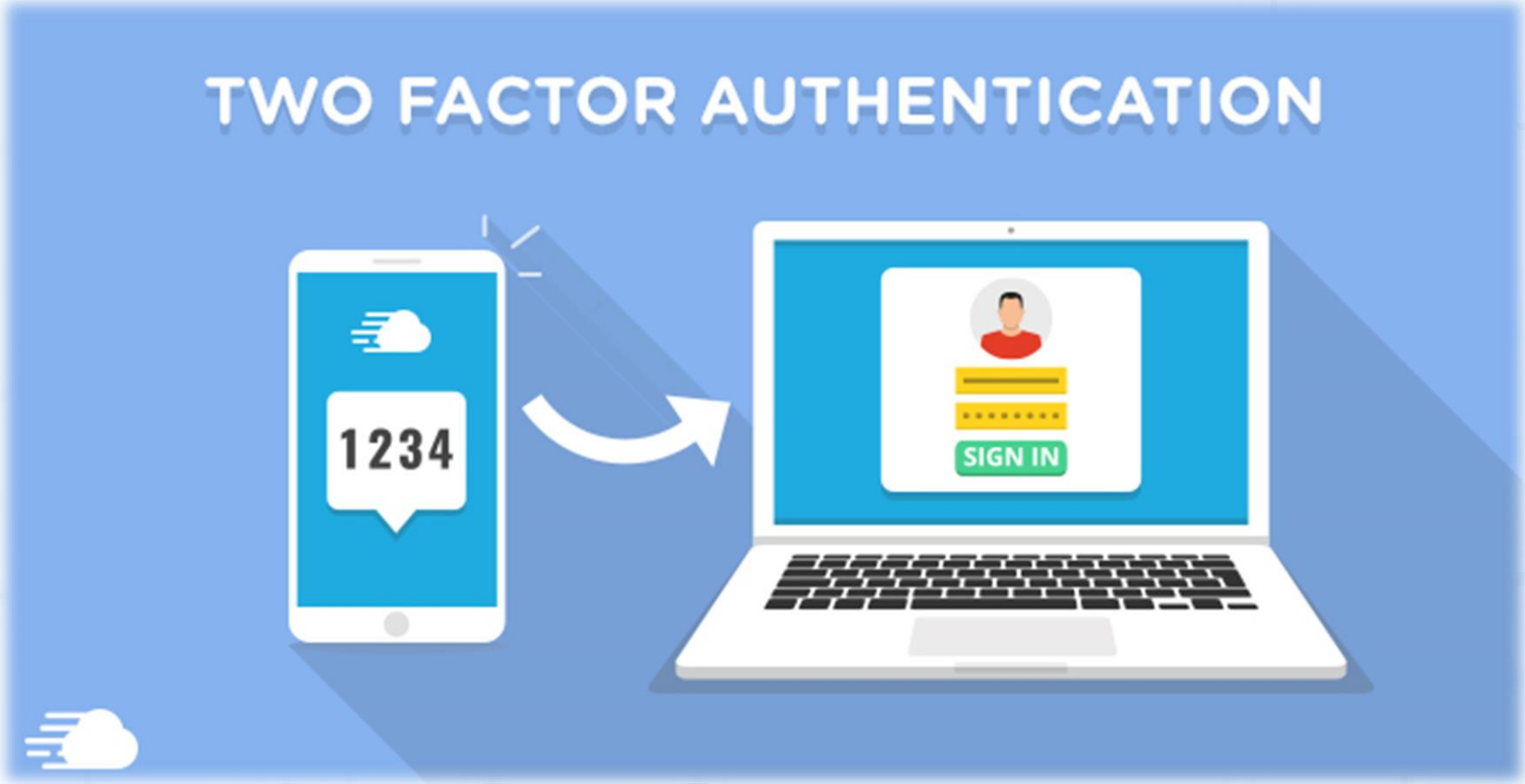
Enforce strong passwords

- The longer, the better
- Check new passwords against a dictionary of known-bad choices
  - NewPassword, Packers, Brewers

Use password management tools

LastPass •••|

Password Security




80%
of hacking attacks could be prevented by strengthening passwords and installing software patches
PCISSC.org/SmallMerchant

Principle of Least Privilege (POLP)

- Conduct an audit and then review regularly
- Create accounts with least privileges, adjust as necessary
- Implement/enforce separation of privileges
- Monitor activities

Education

Training

- Company and Personal Liability
- Identify Social Engineering
- Physical Data Handling Best Practices
- Internal Policies and Procedures

Regulations

- Regulatory Requirements
- New or Changing Regulations

Third Party Assistance

- Guidance on creating a right-sized security program
- Implement a strong data governance/stewardship program
- Manage your security program
- Provide developer training

External, unbiased perspective:

- Penetration Testing
- Remediation Assistance
- Audit
- Measure existing security program

Thank You!

Christy Pernitzke

Phone

262-780-0380

Email

cpernitzke@syslogicinc.com