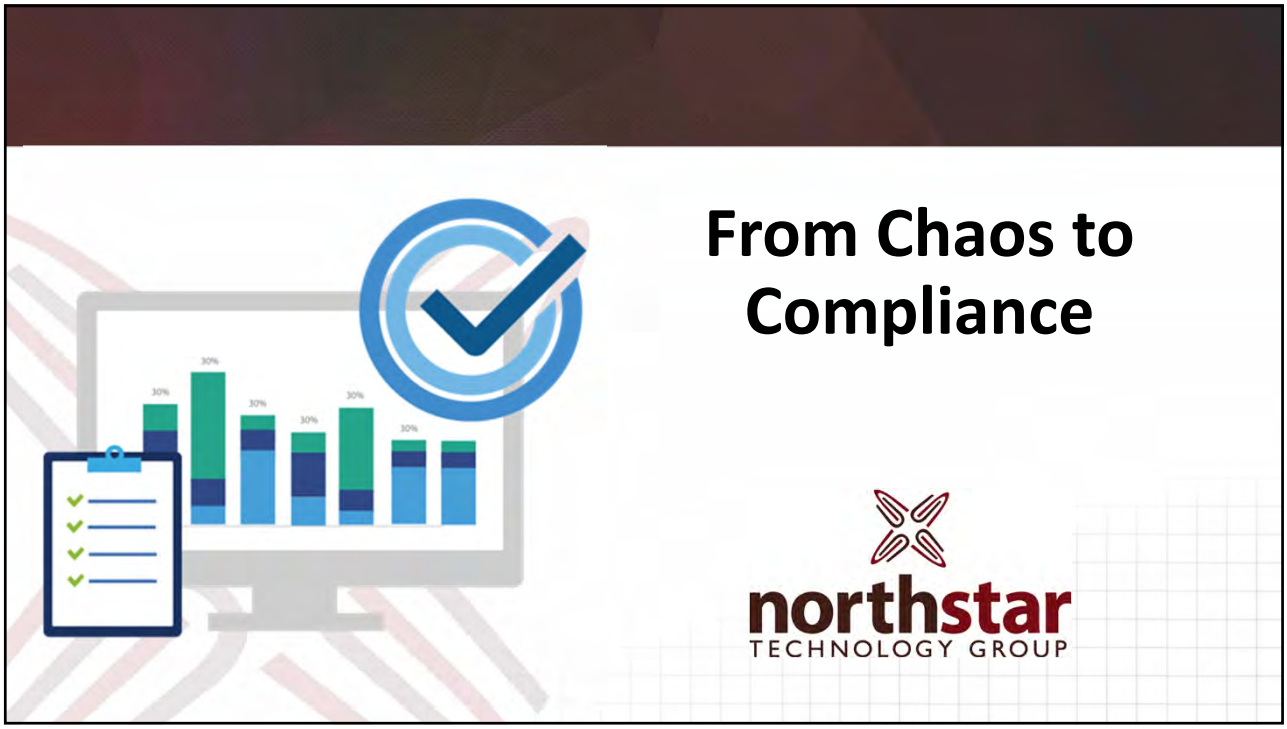


1

I GOOGLED MYSELF…

HIPAA
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

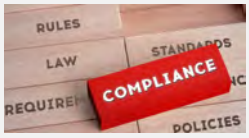
Wellpoint – shared health plan member info on web portal

Skagit County, Washington – accidently published patient info on the web.

NY and Presbyterian & Columbia University Medial Center – Accidently published patient information.

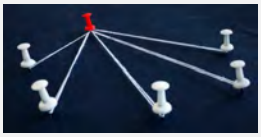
2

KEY TAKEAWAYS – NOT JUST REGULATORY!



The Driving Force Behind Drastic Data Privacy & Cybersecurity Regulations

Why Compliance Should Be A Top Priority For Your Business



Leveraging The Power Of Process Automation

Achieve & Maintain Continuous Compliance

3

WHAT IS COMPLIANCE?

DEFINITION:

Conformity, accordance, cooperation, or obedience

IN PRACTICE WITHIN YOUR BUSINESS:

To comply with the rules, laws, and mandates of applicable regulatory bodies or standards

4

– WHAT IS COMPLIANCE?

MYTHS:

You only need to protect the system that holds the protected data (PII, PHI)

All of your protected data is stored on your servers

Your systems are in the cloud so you don't have to worry about compliance or security

FACTS:

Nearly all of our assessments find protected data stored somewhere OTHER than servers.

All protected data needs to be protected and you connect to cloud services from local devices.

Just because you downloaded policy templates, does not mean you are compliant!

5

– WHAT IS COMPLIANCE?

Lessons:

Compliance is complex. Eat the elephant one bite at a time

Compliance is also defined at the local level – know your local laws

It typically takes about 50 steps to secure your technology, but those steps cannot all be done by your IT team! Get involved!

6

GROWING LIST OF COMPLIANCE REGULATIONS:

7

Executive Order on Improving Cybersecurity:

8

CONSUMERS DEMAND

DATA PRIVACY & SECURITY

DATA PRIVACY

Governs the rules and parameters regarding how and why a consumer's personal data is collected, used, stored and shared, as well as definitively declares the consumer's ownership, rights, and control of their personal data.

DATA SECURITY

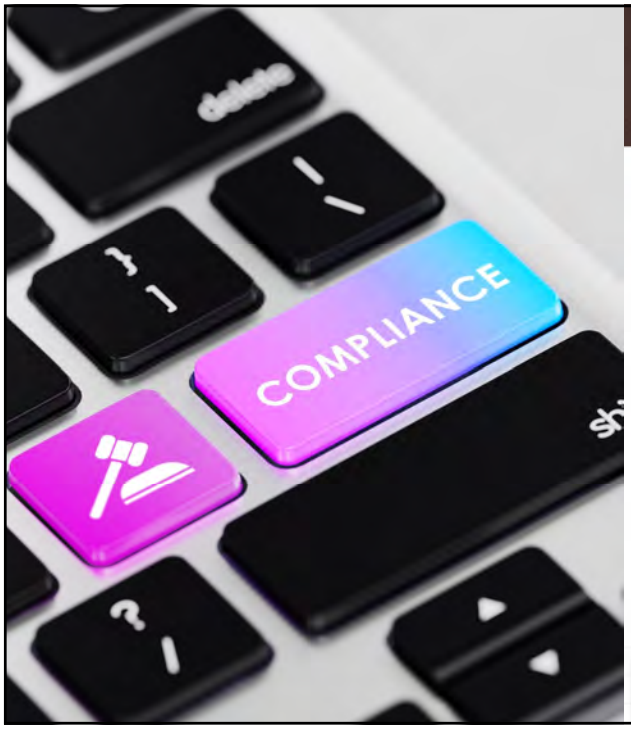
Governs the protection and security of personal data from both external attackers and insider threats against risks such as misuse, loss or theft, and exposure.

9

THE BURDEN OF COMPLIANCE OBLIGATIONS

- Rapidly increasing influx of new regulations
- Existing rules and requirements change regularly
- Producing evidence or proof is mandatory
- Challenges for monitoring compliance in the supply chain
- Tackling new and rapidly evolving cyberthreats
- Limited or scarce resources (time and money)
- Maintaining regular, up-to-date compliance training
- Designating a Compliance Officer/ Manager

10



IT'S THE LAW – NOT OPTIONAL

Regulatory agencies around the world are putting pressure on businesses to establish a more proactive approach to compliance regarding data privacy and cybersecurity best practices.

By ignoring or neglecting these legal mandates, you open your business up to the increased risk of an audit, hefty violation penalties, potential litigation and severe reputation damage, which could lead to a loss of trust and ultimately a loss of customers.

11

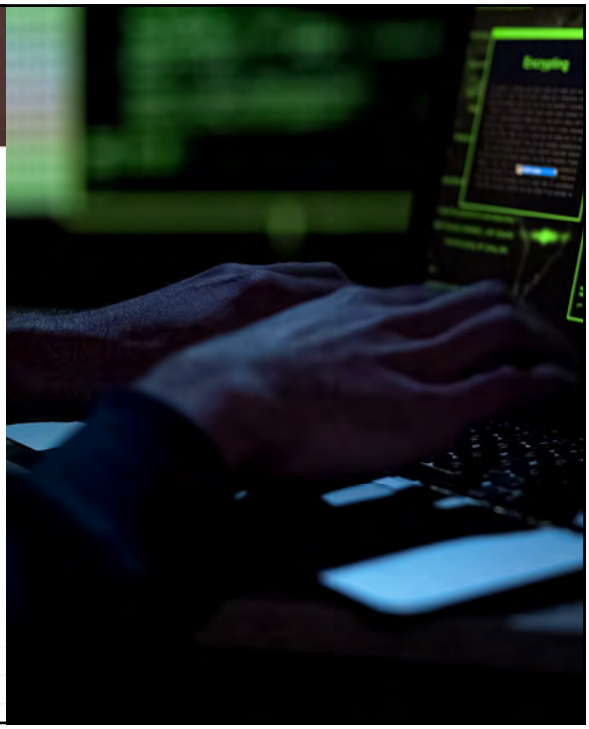
EVOLVING CYBERTHREATS

Compliance and cybersecurity are equally crucial systems to all businesses. While both include several core components, which may align or overlap, neither system individually completely fulfills or eliminates the necessity for the other.

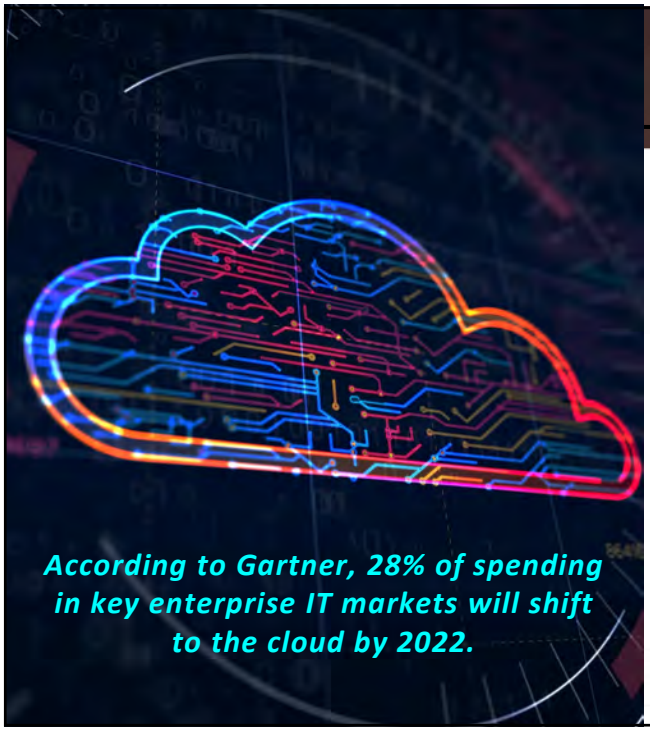
$6T *projected damage related to cybercrime annually by 2021*

95% *of all medical and healthcare institutions have been victims of some form of cyberattack*

43% *of breaches in 2019 involved small business victims*



12



INCREASED RELIANCE ON THE CLOUD

Cloud-based solutions offer flexibility and opportunities for massive growth. However, the Cloud inherently comes with increased vulnerability or exposure to new, rapidly-evolving and sophisticated cyberthreats on multiple fronts.

- ✓ **Unauthorized Access**
- ✓ **Data Breaches, Leaks, or Theft**
- ✓ **Data Corruption or Loss**
- ✓ **Insecure APIs**
- ✓ **Misconfigured Applications or Storage**

13

PITFALLS OF NON-COMPLIANCE

REGULATORY PENALTIES	EXPENSIVE LAWSUITS	PR FALLOUT	LOSS OF PUBLIC CONFIDENCE
LOSS OF SHAREHOLDER VALUE	INCREASED GOVERNMENT OVERSIGHT	DIFFICULTY RAISING CAPITAL	POSSIBLE LICENSE SUSPENSION

14

AH [2]7

STEP 1 - RISK ASSESSMENTS AND REMEDIATION

Compliance risk is the risk of facing legal or regulatory sanctions, financial loss, damage to reputation, or worse - a security breach courtesy non-compliance. Building a comprehensive framework for regular assessment of compliance risk is mandated by nearly all regulatory standards.

Regulatory Matrix → Compliance Risk Analysis → Continuous Compliance Management

15

TECHNICAL AND ADMINISTRATIVE SAFEGUARDS

ACCESS & AUDIT CONTROL
Ensuring each activity can be traced to a user and mechanisms are implemented to examine activity in information systems.

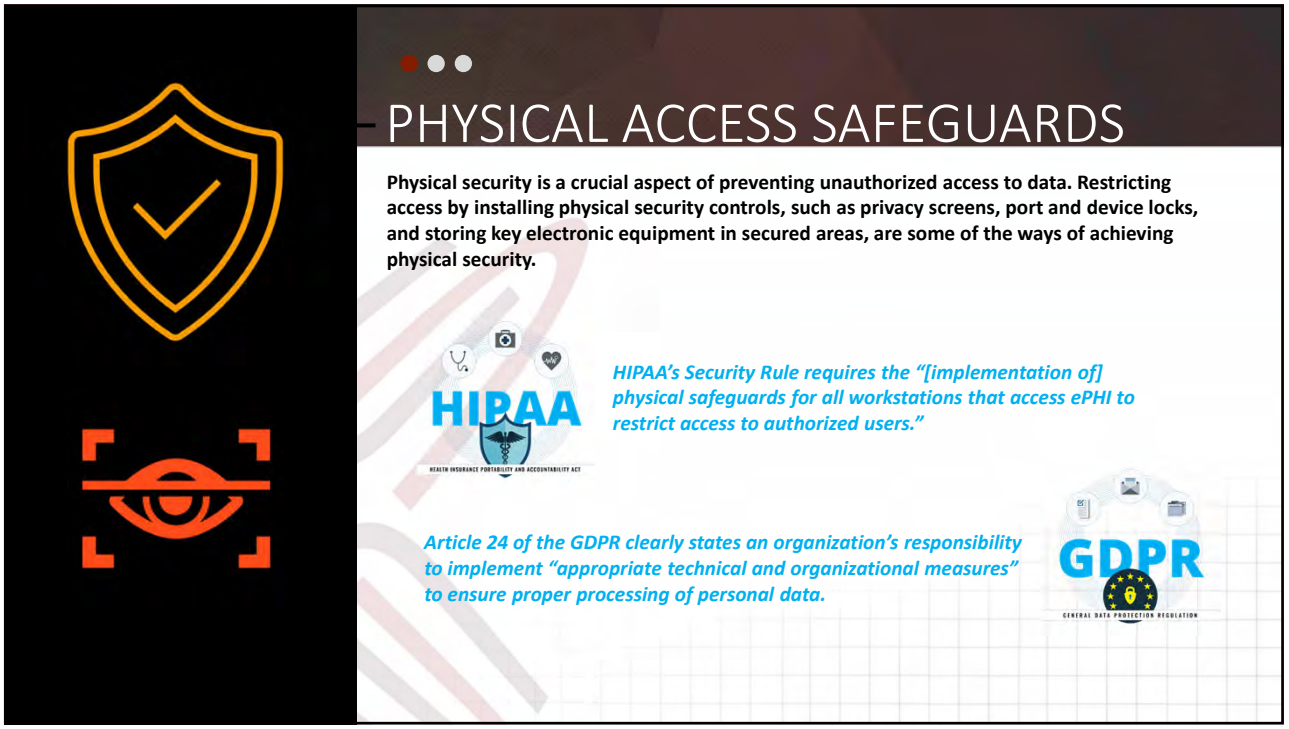
AUTHENTICATION & INTEGRITY
Authenticating user identities and protecting data from improper alteration or destruction.

INCIDENT REPORTING
Establishing a mechanism to report a security breach as per the mandated guidelines.

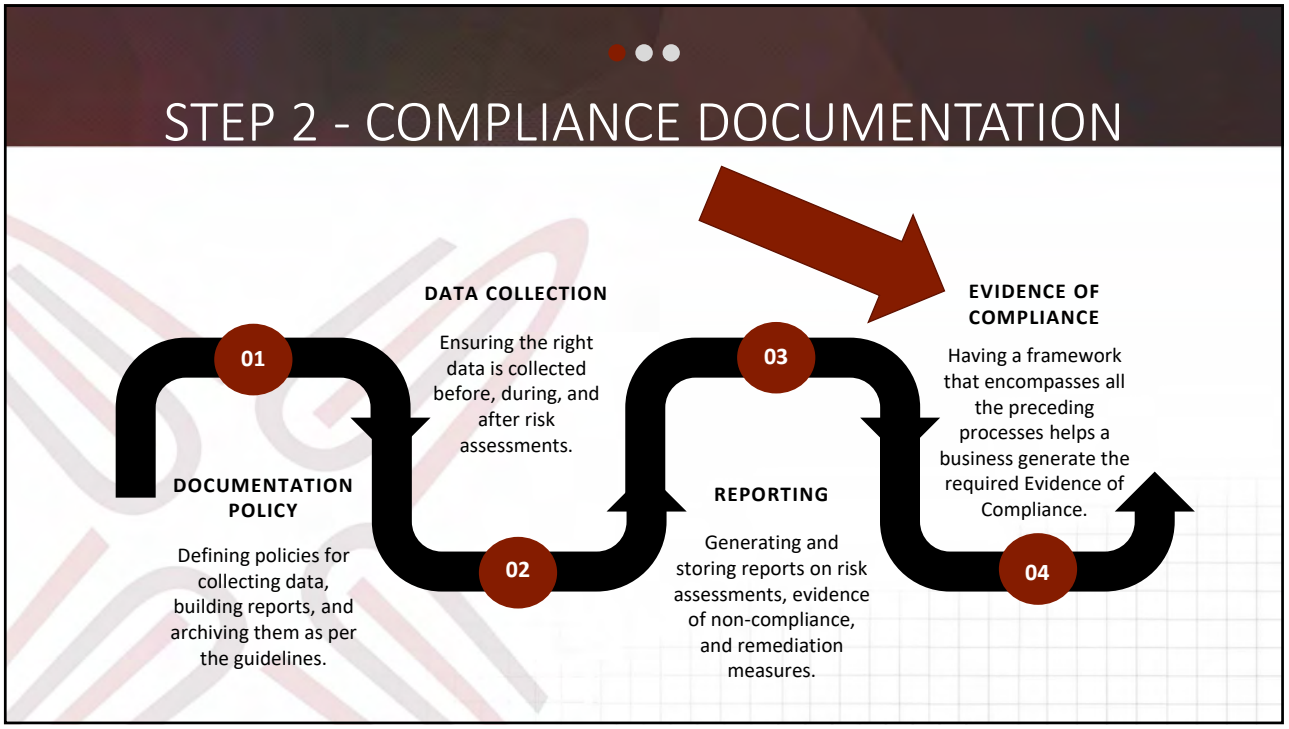
16

Slide 15

AH [2]7 Need to understand the descriptions for the 3 components and how they are relevant
Ashley Harris, 7/20/2020


PHYSICAL ACCESS SAFEGUARDS
Physical security is a crucial aspect of preventing unauthorized access to data. Restricting access by installing physical security controls, such as privacy screens, port and device locks, and storing key electronic equipment in secured areas, are some of the ways of achieving physical security.
HIPAA
HIPAA's Security Rule requires the "[implementation of] physical safeguards for all workstations that access ePHI to restrict access to authorized users."
Article 24 of the GDPR clearly states an organization's responsibility to implement "appropriate technical and organizational measures" to ensure proper processing of personal data.
GDPR

17


STEP 2 - COMPLIANCE DOCUMENTATION
01
DOCUMENTATION POLICY
Defining policies for collecting data, building reports, and archiving them as per the guidelines.
02
DATA COLLECTION
Ensuring the right data is collected before, during, and after risk assessments.
03
REPORTING
Generating and storing reports on risk assessments, evidence of non-compliance, and remediation measures.
04
EVIDENCE OF COMPLIANCE
Having a framework that encompasses all the preceding processes helps a business generate the required Evidence of Compliance.

18

STEP 3 - LEVERAGING PROCESS AUTOMATION

Simplify the compliance process with automated data collection and analysis that enables your organization to quickly produce audit and change logs, remediation records, and other mandatory documentation and reports that demonstrate and satisfy Evidence of Compliance.

- ***Asset discovery, non-compliance apps, user privileges and access***
- ***Ongoing monitoring, activity logging, off-site/remote system monitoring, reporting***
- ***Patch management, password management, virus/malware scans, unusual activity or user behaviors***

19

THE BUCK STOPS WITH YOU!

The responsibility of ensuring compliance rests with YOU. No finger pointing allowed.

Your vendors may share fault or blame, but when it comes to compliance, it doesn't lessen your responsibility in any way.

20

WILL INSURANCE SAVE YOU?

Cottage Health

21

ACHIEVE & MAINTAIN CONTINUOUS COMPLIANCE

Compliance is not a one-and-done exercise - it requires sustained effort.

RISK ASSESSMENTS
Conducted regularly as and when needed (quarterly, semiannually, annually).

REMEDIATION
In order to resolve all vulnerabilities and missing obligations.

DOCUMENTATION
Produce and maintain mandatory reports regularly to demonstrate "best efforts"/"due diligence" during an audit.

MAINTENANCE
Routine vulnerability scans, appropriate reporting, and updated documentation.

22

LESSONS LEARNED

- ✓ **Get a security risk assessment done ASAP!**
- ✓ **Get a good E and O + Cyber policy**
- ✓ **Compliance is not just an IT responsibility – get involved!**
- ✓ **Implement basic security best practices RIGHT NOW.**
  - ✓ **Encrypt all of your devices**
  - ✓ **Implement multi factor authentication**
  - ✓ **Implement email security to protect from viruses and phishing**
  - ✓ **Train your employees on security awareness**
  - ✓ **Use software and people to analyze security logs (SOC and SIEM)**
  - ✓ **Use password managers to allow for complex passwords**
  - ✓ **Create policies and procedures around all of these things that you can enforce**

23

PARTNER WITH A SPECIALIST

- ✓ **Detect** your compliance needs and vulnerabilities with a comprehensive risk assessment.
- ✓ **Automate** data collection, analysis, and documentation processes.
- ✓ **Identify** appropriate remediation measures and highlight critical items or issues needing immediate attention.
- ✓ **Provide** expert technical support and guidance you can put your trust in.
- ✓ **Secure** and protect your business and its data from new or evolving threats and sophisticated cybercriminals.
- ✓ **Generate** detailed records and reports to demonstrate and validate Due Care or Evidence of Compliance requirements.
- ✓ **Deliver** and manage all the above for a variety of regulatory standards with our simple, budget-friendly CaaS solution.

24

PARTNER WITH A SPECIALIST

Ken.Satkunam@northstar-tg.com

Linkedin.com/in/kensatkunam

Facebook.com/ken.Satkunam

www.northstartechnologygroup.com