Managing Cyber Security Risks

Overview & Best Practices

Presented By:

Speaker Info

Steve Smith, CPCU, AIM, RPLU

The Cincinnati Insurance Companies
National Program Director
Social Services, Hospice and Home Health Care
Steve_Smith@CINFIN.com

Randy Steinle

Cyber Trust Alliance
CEO, Co-Founder
rrsteinle@cybertrustalliance.com

THE CINCINNATI INSURANCE COMPANIES

- Property and casualty insurance carrier founded in 1950
- AM Best Rating of A+ and an overall rating of A or better for 50 consecutive years
- Coverages specifically designed to meet the needs of adult day services organizations as well as a variety of other businesses and organizations.

CYBER TRUST ALLIANCE

Cyber Trust Alliance reduces risk, saves money and simplifies compliance for healthcare organizations.

CEBA Risk Management Suite

CEBA COMPLY *Simplified Compliance/Reduced Risk*

CEBA LEARN *Training and Learning Management*

CEBAVENDOR *3rd Party Risk Management*

CEBA FOLDERS *Policy/Document/Contract Management*

CEBA PHISH *Phishing Assessment and Training*

Session Objectives

At the completion of this program, the participant will be able to:

- ❑ Understand today's cyber threats and risks
- ❑ Understand the law regarding security and privacy compliance for healthcare
- ❑ Have a better understanding of practical tools, techniques and solutions to help reduce and manage risks to your business including:
  - Cyber Liability Insurance
  - Cyber Security Solutions
  - Education
  - Ongoing monitoring and documentation of your efforts

Compliance and the Law

HIPAA SECURITY

45 CFR Part 160 and Part 164, Subparts A and C

The Security Rule requires covered entities (healthcare providers) to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

HIPAA PRIVACY

45 CFR PART 160 AND PART 164, SUBPARTS A AND E

The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.[1]

HIPAA BREACH NOTIFICATION RULE

45 C.F.R. PART 160 , PART 162, AND PART 164

"This federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care."

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Polling Question

How many patient records were breached in 2022?

- 15.3M
- 26.7M
- 59M
- 67.2M

Lack of HIPAA compliance cost healthcare $29B in 2023

59M *healthcare records breached in 2023 in the US*

$29B *total cost of breached healthcare records*
(@$499/record = 3x higher than all other industries)

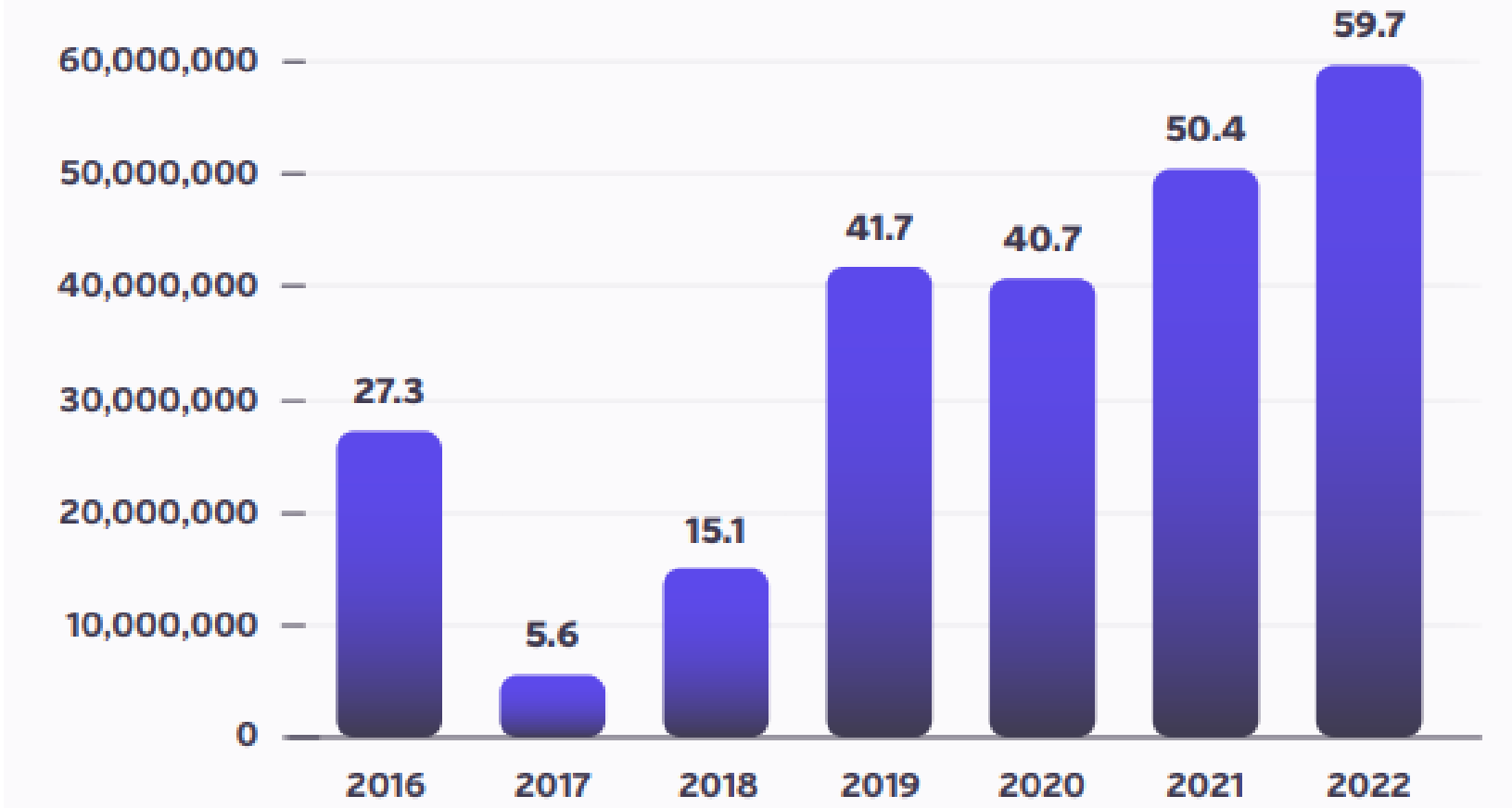
And Yet . . .

2023 Breach Barometer®

A look back at 2022 and insight on what 2023 could hold for healthcare data breaches

Figure 2.

Total breached patient records, 2016-2022 health data breaches

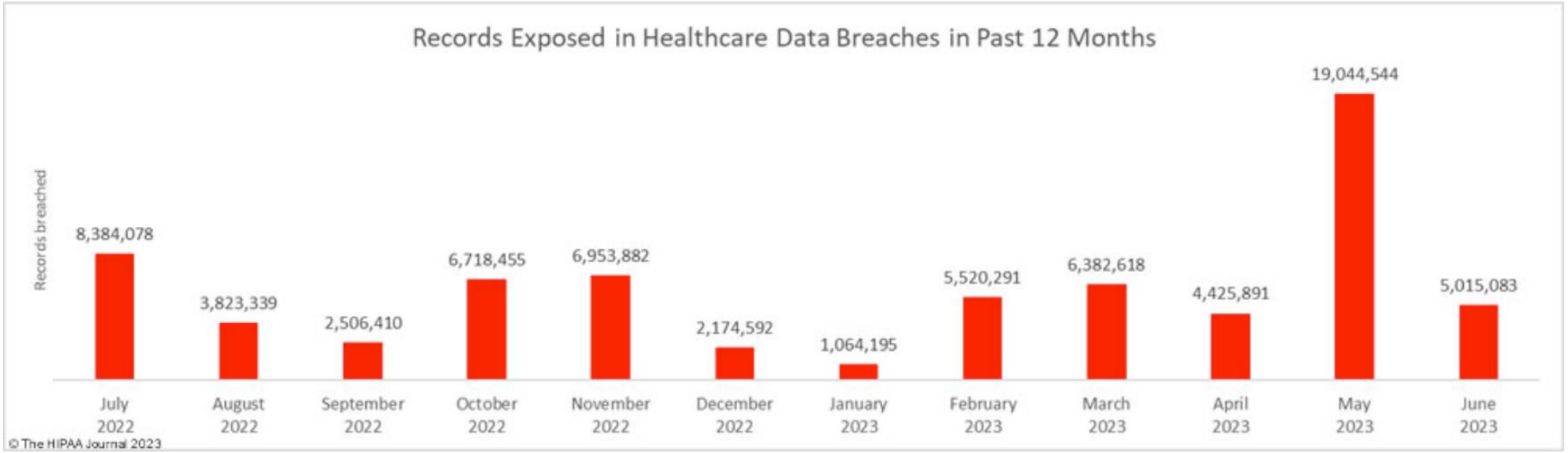


More than 59.7 million patient records breached as hackers redouble efforts in a challenging climate

PROTENUS®

In collaboration with DataBreaches.net

41M Healthcare Records breached 2023



In H1 2023, 41,452,622 healthcare records were exposed or impermissibly disclosed. That's just a few thousand records short of the total for all of 2019 and just 10 million below the total for all of 2022.

June 2023 Healthcare Data Breach Report THE HIPAA JOURNAL

Posted By Steve Alder on Jul 20, 2023

Polling Question

How much does a breached healthcare record cost the provider?

- $141
- $235
- $499
- $679

Bonus Question

On average, how much does a breached healthcare record cost the patient?

- $2,000
- $12,000
- $20,000
- $32,000

Why is Healthcare a Prime Target?

1. Private patient information is worth a lot of money to attackers
2. Medical devices are an easy entry point for attackers
3. Staff need to access data remotely, opening up more opportunities for attack
4. Workers don't want to disrupt convenient working practices with the introduction of new technology
5. Healthcare staff have numerous patient-focused priorities over keeping current on online risks
6. The number of devices used in hospitals makes it hard to stay on top of security
7. Healthcare information needs to be open and shareable
8. Smaller healthcare organizations tend to have fewer protections
9. Outdated technology means the healthcare industry is unprepared for attacks

9 Reasons Healthcare is the Biggest Target for Cyberattacks (swivelsecure.com)

Polling Question

What percentage of cyber attacks target small businesses?

- 52%
- 26.7%
- 74%
- 98%

Who is being targeted?

Key Findings

Company Size

This year's report continues a painful trend as it starts to hit the mathematical extremes of the prior studies. The attacker's shift in preference to small and mid-sized organizations has become overwhelming, where the data shows that being an organization of specific size is more dangerous than being in a specific industry. The only universal constant across both large and small organizations is that incident costs continue to increase and actually appear to be accelerating.

Daimon Geopfert
National Leader,
Security and Privacy Services
RSM US

Source: NETDILIGENCE® CYBER CLAIMS STUDY 2020 REPORT

Small to Medium Enterprise (SME)

Categorized in this study as organizations with less than $2 billion in annual revenue.

Risk Management

GOAL:

Reach a state of ***CYBER RESILIENCE*** in which you can properly identify, respond, and recover from a Cyber Incident.

1. **Identify** Assets (information, objects) Threats (physical and electronic)
2. **Analyze** Threats in relation to assets, considering vulnerabilities and controls. Asset +Threat + Likelihood + Impact = Risk
3. **Plan** remediation (Avoidance, Transference, Acceptance)
4. **Monitor** for threat activity, emergence of new threats
5. **Respond** to threats and changes internally and externally (threat landscape)

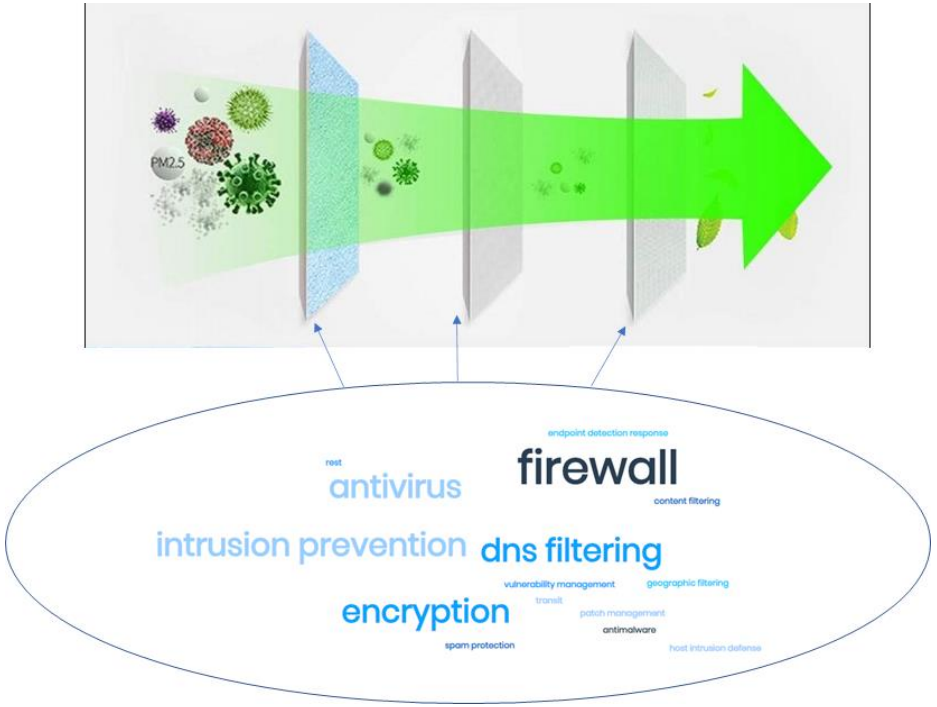
Compliance Is:

a) Minimum necessary standards
b) Designed for awareness and education
c) The Starting Point

1. **Identify Risks**
   - Identify existing and new/emerging threats
   - Identify existing and new/emerging vulnerabilities
2. **Analyze Risks**
   - Assess and Analyze threats and vulnerabilities
3. **Plan**
   - Create a Plan for Remediation
4. **Document**
   - In Compliance – if it's not documented, it never happened
5. **Train**
   - Human beings are often the weakest link in a cyber security/compliance program
6. **Repeat**
   - Compliance is not a destination – it's a journey – new threats are discovered every day
   - Bad Actors aren't taking a day off – neither can we

Cyber Security & IT

- Cyber Security is not one-size fits all – nor is a single solution/approach adequate.
- Good Cyber Hygiene requires layered security to address and "filter out" increasingly challenging threats and vulnerabilities



Cyber Security & IT

Biggest threats:

- Email – Phishing
- Browsing – Sites with Malicious Software
- Out of Date Software
- Hacking
- Employees – Lack of Training

Why Does It Matter?

- **Ransomware/Encrypted Systems**
  - Costs money, time and reputation
- **Stolen Data**
  - Patients get identities stolen – lose trust
- **Installed Malware/Viruses**
  - Compromised credentials – access to data

Cyber Security & IT

What Can You Do?

- **Implement Multi-Factor Authentication**
  - ✓ **Identity and Access Management** - **Protect your identity at all times**
- **Configure Email Protections:**
  - ✓ **SPF, DEMARC, DKIM** - Put simply, these antispam measures verify that a sender is legitimate and that their identity has not been compromised.
  - ✓ **SPAM Filtering** – Proactively identify threats in emails and email attachments
- **Design and Configure Browser Protections**
  - ✓ **Content Filtering** – manage the sites and content your staff accesses
- **Train Staff**
- **System Updates and Patching**
  - ✓ **Apply Software Updates and Patches** - Software vendors release updates and patches to address new vulnerabilities – if you don't apply these regularly, your systems will be unprotected.
- **Data Backup and Disaster Recovery**
  - ✓ **Segregated and Offsite** to prevent tampering/ransomware
  - ✓ **Tested Regularly**
  - ✓ **Failover for Disaster Recovery**
- **Monitor**

Cyberattacks are business-disrupting events!

Cyber insurers today are no longer in just the loss recovery business for their insureds. They are in the business now of embedding risk management to make an insured's cybersecurity posture more robust.

What is Cyber Insurance

Cyber Insurance covers the economic or legal costs arising out of a Data Disclosure or Network event.

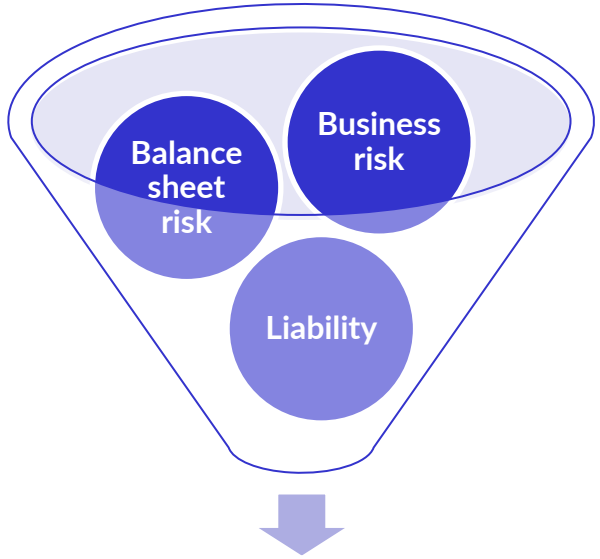
- Offers both services & financial risk transfer.

INCIDENT RESPONSE: To determine what happened, how to repair the damage, to reduce downtime and to meet privacy regulatory requirements. Includes IT Forensics, Legal, PR, and notification costs.

LAWSUITS & PRIVACY REGULATORY INVESTIGATIONS: Legal fees, legal settlements and also regulatory fines where insurable (such as HIPAA, PCI, GDPR, CCPA, etc violations)

CYBER CRIME: Costs such as ransom or extortion payments, phishing, and social engineering.

BUSINESS LOSSES: Impact to operations or ability to generate revenue both during an incident and afterward as it impacts your reputation.



Cyber Insurance – Top Coverage Considerations

1) **Adequacy of Limits**

2) **Dependent System or Outsourced Provider – Business Interruption**
   - Waiting period

3) **Reputational Harm**

4) **Social Engineering – Limits & Restrictions**

5) **Cyber Crime**

6) **Workforce Security Training**

Cyber Insurance – Coverage options

BREACH RESPONSE EXPENSES AND SERVICES

- Breach expenses
- Defense and liability
- Identity recovery for owners and key employees
- Forensic IT and legal review sub-limits
- Regulatory fines
- Public relations expenses

COMPUTER ATTACK COVERAGE

- Data restoration
- Data re-creation
- System restoration
- Loss of business income
- Public relations services
- Network security liability
- Other
  - Cyber extortion
  - Electronic media liability

Cyber Insurance - what next?

- **Insurance Rates Increasing & Coverage Limitations Spreading**
  - Consider buying higher limits, while it is still affordable!
  - Coinsurance on Ransomware
  - Specific Cyber Event exclusions

- **Insurance Carriers starting to mandate more security requirements**
  - Multi-Factor Authentication
  - Segregated Backups
  - Endpoint Detection & Response

- **Continued increase in the Frequency & Severity of Claims**

- **Increase in Regulation**

Polling Question

What one (1) cyber security initiative from the list on the previous page should you commit to implementing this quarter?

Reference Materials

Patch Now!

CISA warning: Hackers are exploiting these 36 "significant" cybersecurity vulnerabilities - so patch now - The United States Cybersecurity and Infrastructure Agency (CISA) has added 36 new flaws to its catalog of vulnerabilities that are known to be exploited by cyber criminals.

The CISA alert warns that the vulnerabilities are a frequent attack vector for malicious attackers and pose **"significant risk".**

"CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of catalog vulnerabilities as part of their vulnerability management practice," said CISA.

https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/cisa-warning-hackers-are-exploiting-these-36-significant-cybersecurity-vulnerabilities-so-patch-now/

source: ZDNet – June 9, 2022

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

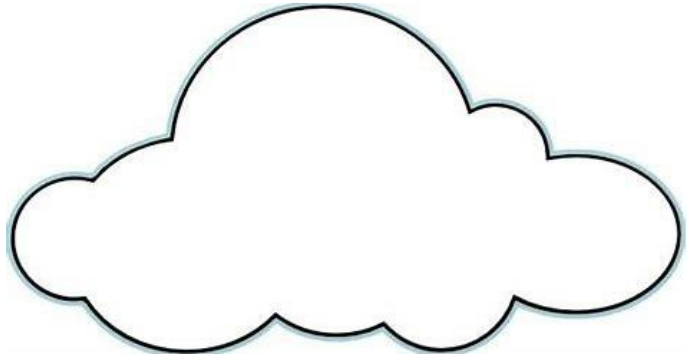
Free resources to help!

- Created in 2018, CISA is a division of the United States Department of Homeland Security

- Locations throughout the country provide businesses and organizations with resources and tools to build their own cyber, physical and communications security

- Regional offices will provide on-site assessments of your cyber exposure at no cost to you; visit CISA Regions on www.cisa.gov to find a location near you

I’m in the Cloud so I’m compliant and secure, right?



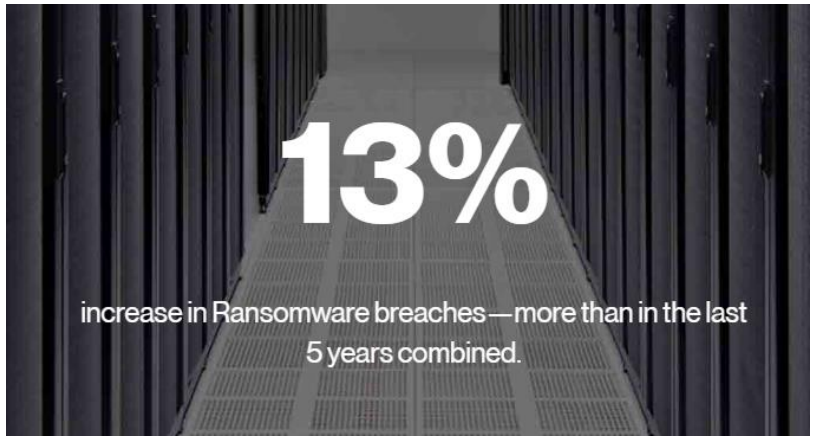
Cloud computing dominates. But security is now the biggest challenge

- Cloud computing has some obvious advantages; but the switch to cloud computing also brings new challenges. And the biggest worry for many is security.
- While the move to cloud computing may have removed some basic security worries, the emergence of the hybrid cloud has introduced a whole new set.
- No two cloud services are exactly the same, and the risks increase as the use of cloud computing expands to new areas.

Cloud computing dominates. But security is now the biggest challenge | ZDNet

source: ZDNet – June 1, 2022

Verizon 2022 Data Breach Investigation Report



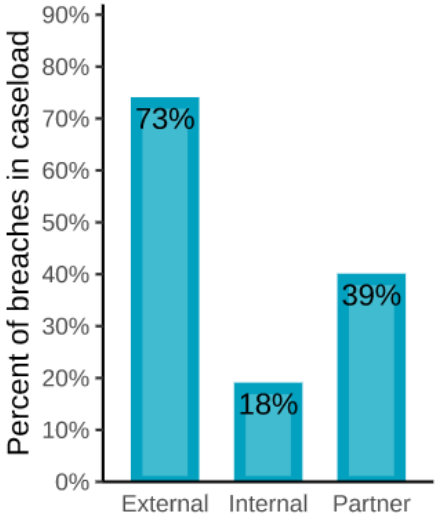


Figure 10. Sources of Data Breaches (2008 DBIR Figure 3)

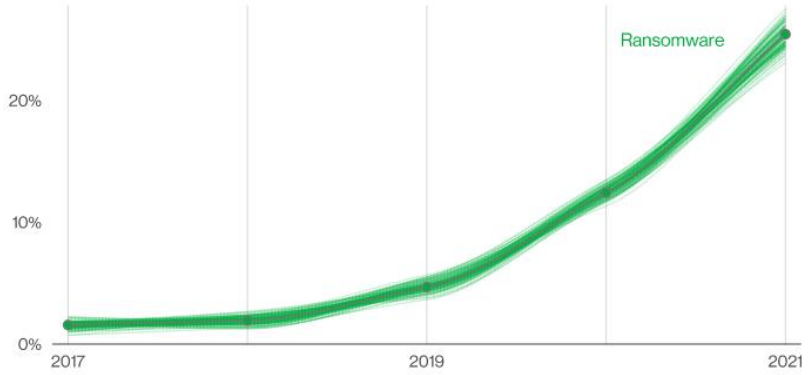


Figure 38. Ransomware over time in breaches

source: [2022 Data Breach Investigations Report | Verizon]

Cybersecurity Authorities Issue Advisory

Cybersecurity authorities from the US, the UK, Canada, the Netherlands, and New Zealand outlined common practices that threat actors use to gain initial access to victim networks.

"Cyber actors routinely exploit poor security configurations, weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system,"

- The statement highlighted a simple truth—**threat actors do not necessarily need elaborate and sophisticated tactics to successfully take advantage of victims**.
- Addressing common security weaknesses and implementing a robust security architecture can help organizations effectively mitigate cyber risk.
- **Specifically, the authorities identified the following five commonly used hacking techniques:**
  - Phishing
  - Exploiting public-facing applications (patient portal, payment portal, etc.)
  - Manipulating external remote services (VPNs, remote desktops, etc.)
  - Gaining access to valid accounts
  - Leveraging trusted relationships
- The advisory stressed the importance of multi-factor authentication (MFA) to prevent account takeovers.

source: Cybersecurity News – May 17, 2022) - Cybersecurity Authorities Issue Advisory on Common Initial Access Tactics (healthitsecurity.com)

Q&A

Steve Smith, CPCU, AIM, RPLU

The Cincinnati Insurance Companies
National Program Director
Social Services, Hospice and Home Health Care
Steve_Smith@CINFIN.com

Randy Steinle

Cyber Trust Alliance
CEO, Co-Founder
rrsteinle@cybertrustalliance.com
(512)680-2442