Converge23 **Speaker Notes**: Cybercrime Crashes into Compliance

Brian Allison May 17, 2023

Converge23 Cybercrime Compliance May2023 v02.docx

1. **Agenda**, brief bio, 20 minutes of talk, 5 for Q&A. Let's go!
    a. Use conglomerations of data, mileage varies, this is consensus as judged by me. Sources are US Government and therefore freely available. Images are licensed for use.
    b. What is the business landscape
    c. What is the threat from cybercrime
    d. What is the impact on business - money
    e. Risk Management and Protection
    f. How that risk is driving compliance
2. **LANDSCAPE Data is the new oil –** The modern Treasure Chest for a modern business - It runs on data, and the data defines the company. We can recover the apps all we want, it's worthless without your data. Your data is your businesses lifeblood.
    a. How far has this gone? More than half the global economy is digital mission-critical.
        i. My background, OEM to Banking & Burroughs: Mission-critical means directly required to earn revenue.
    b. "How many of you in public practice did a paper return for 2022 taxes?" I've run into family businesses that have been in operation for 30-40 years, and they started on paper, but they can't go back.
3. **Business runs on data**
    a. And not the other way around. Historically, the folks that sign the checks don't love technology, it's a necessary cost-center. That thinking is outdated. Technology defines how you service clients, efficient and effective.
4. **Client service wins**
    a. Herb Kelleher - said this about Southwest Airlines **"We're a customer service company** that happens to be in the airline business."
        i. Every business is a service business at the end of the day.
    b. Proper business app drives seamless client support – the rep knows the status, is empowered to take action.
5. **Every company is a tech company.**
    a. How a company applies tech to their **mission-critical workflow** determines a competitive advantage – efficiently provide and track customer service.
    b. Economists generally believe that more than half of GDP is now digital mission-critical
    c. "How many of you in public practice did a paper return for 2022?
6. **There Be Pirates (treasure chest)**

a. They want the treasure as always
b. Pirates are malware as a service, running as a tech company.
c. Devs, marketing, customer service-how to pay them in Bitcoin.
d. Revenue-sharing distribution channels through affiliates
e. Smart, talented people
f. Who pays a large component of their revenue?

7. **Defend the ship**
    a. **Cybersecurity is integral to mission-critical operations.**
    b. Black Hats against White Hats.
        i. White Hats are cybersecurity providers,
            1. Very intensive tech businesses-software-driven
    c. Arms race, Continuous innovation
    d. Santa Clara police and 10-foot wall, 11-foot ladder
8. **Infosec = CIA (CIA logo)**
    a. Not that CIA – you guys in the van outside, you caught that right?
    b. Confidential – only you have it, no one else
    c. Integrity – the data is reliable and trusted, not tampered with
    d. Available – no fair unplugging it
9. **Cost >> Income**
    a. **- Victim Cost >> Criminal Income,**
    b. like 10-1 or even higher
    c. Means loss to the business are a significant risk
10. **UBIQUITI EXAMPLE,**
    a. CEO to Asia, posted on LIn,
    b. BEC spoofing cost them $47 million, $15 Million clawed back.
11. **FAKE POOJIT**
    a. Global 200 company, 300K employees, $70 billion revenue gained access to his email, spoofed history, gave instructions to the CFO to change payment address with an email from a project manager,
    b. Used a US bank and it was clawed back.
12. **Law Firm Real Estate closings**
    a. 2nd: Old lady had her email compromised, which pivoted to sending her a fake email from real estate closing lawyer, money not recovered. $1 million. Transaction completed next week with a fresh million.
13. **Targeted based on process maturity**
    a. not just industry – more sniper, less shotgun.
    b. Organizations are targeted because they made poor tech choices.
    c. We don't need that kind or protection, we're too small." Maybe not anymore
14. **Risk Management**
    a. **significant component of these costs are born by commercial insurance**
    b. payouts above 70% of premiums, exceeding the break-even point
    c. something has to give

15. **Compliance - Time and Money (stopwatch and phat stack)**
    a. **Compliance is expensive**
    b. **to be avoided -** Time and money, distraction, opportunity cost
    c. Continuous commitment – not once and done
    d. Externally imposed by law
16. **HIPAA (medical doctor)**
    a. What is compliance? HIPAA, PCI (PCI-DSS), FINRA and many others in investments are best examples, associated with your industry - important
    b. Organization offers positive affirmation, with details, that they are following specified practices. Covers all the things you're supposed to do
    c. Subject to regular review of actual performance against the standard
        i. Identify the gaps
        ii. Remediation plan to address the gaps,
            1. must be followed,
            2. can't be zero

17. **NIST 800 where did it all come from ( )**
    a. **The OG compliance is NIST 800 docs** How long is a foot, how heavy is a pound
    b. Aimed at Fed agencies, adopted later by industry starting with Fortune 500
    c. Critical infrastructure like power grid and pipelines
        i. Speaking of Pipelines → Colonial pipeline, 10 miles from here
        ii. Ransomed and shut down for a week a couple of years ago
        iii. Panic-buying and long lines at gas stations
        iv. Really 2 Pipes, 100 million gallons a day from Houston to Northern NJ
        v. 10 miles away, leaked 2 million gallons into a nature preserve
        vi. Extreme example
18. **Little ol' me**
    a. Vast majority of US businesses by number are under 25 people
    b. Don't have the resources
    c. Also don't have the risk profile – size, scope, etc.
    d. There is recognition of this fact, so the number of controls is reduced based on size
        i. CIS "Implementation Groups" 1, 2, and 3 (big)

19. What about CPAs?

a. IRS Publication 4557 (Rev. 7-2021, 22 pages) Catalog Number 48905Y Department of the Treasury Internal Revenue Service www.irs.gov
b. Contains a checklist of what to do
c. Biz & Indust CPAs included, also handle taxpayer info
d. IRS Checklist, printed out as a hand-out.

20. What are insurance companies doing now –

a. Providing best practices, biggest one now is MFA on email
    i. Estimated 80-90% of attacks started with email.
b. **Underwriters -** payouts above 70% of premiums
c. Raising premiums, imposing requirements that control risk and feed rating
d. More expensive, maybe refuse to underwrite.

21. Carrier 1

a. Which cloud infrastructure platforms do you use?
b. How do you manage your IT and security infrastructure?
c. Do you enforce MFA?
d. Phish Training
e. **Data** Protection –
    i. how do you use it,
    ii. where is it stored,
    iii. is it encrypted
    iv. who has access
f. Business Continuity/DR Plan?
g. Security in use for computers

i. Beginning of compliance – via insurance, not govt

22. **Carrier 2**
    a. **All the above plus:**
    b. How many PII records & what type? What does your risk profile look like? What are you doing to control risk?
        i. Encryption in use? Policies in place, compliance with HIPAA, PCI-DSS, Fraud controls & type, phish threat training, secure VPN, backup policy-offsite copy
        ii. BACKUP 3-2-1 PLAN: 3 copies of data (1 is production) in 2 different places, 1 of which is offsite.
    c. Biz Cont/DR plan tested at least annually?
    d. 3rd party content properly licensed w/legal review,
    e. Loss history, **any existing threat** that could lead to a claim?
23. **Why MFA**
    a. MOST CYBERCRIMES START WITH EMAIL
    b. Not just ransomware
    c. Also social engineering, phone or in person
    d. This problem won't go away – the attackers are at work every day.
24. **Quote from Jeff Steele**, Wells Insurance Agency, commercial insurance agent
    a. It all started with businesses losing control of PII
        i. Sued by customers isn't a great look – didn't do the bare minimum
        ii. Depending on needs, can be a separate policy or a rider to the commercial one
        iii. Had a 150-employee customer walk away from a good policy over MFA
        iv. Seen some polices go from $5K to $30K, based on risk & controls
        v. Had a client get ransomed, ransom would be covered by policy limits
            1. Threat actor was from Russia
            2. Sanctions didn't allow them to pay legally
            3. Did not have adequate backups to recover, lost their data.
            4. He lost the client
25. **"Tips for Insurance Buyers"** provided to his clients via Wells
    a. Work with a trusted pro
    b. Understand your needs
        i. Pick the best choice
        ii. Carriers offer Loss Control services
    c. User is the last line of protection → educate
        i. "don't fix the user" don't make it punitive, at least at first.
    d. Have a pro-active tech plan – don't wait, it's too late
26. **Shameless Commerce Plug:**
    a. Working set of policies for IG 1 in CIS, available to clients
        i. Mostly standard, one section custom to the business by sector

b. We sell cybersecurity services.
c. Provide referral for cyber insurance.

27. **Q & A**

End speaker notes

----------=----------

NOTES: The defined "controls" in Special Publication 800-53 Latest Revision 5, 492 pages, available free of charge to the public https://doi.org/10.6028/NIST.SP.800-53r5 → Security and Privacy Controls for Information Systems and Organizations
This is the OG standard for Cybersecurity, originally targeted at fed agencies.
Companion doc: Cybersecurity Framework 1.1, "Framework for Improving **Critical Infrastructure** Cybersecurity," available for free at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf Gives details, recognizing that industry is mission-critical for our daily lives, and cybercrime is a threat.
History - Colonial pipeline - supplies nearly half of the fuel for the East Coast, gas/av gas/heating oil from Texas refineries. Fear of a gas shortage caused panic-buying and long lines at gas stations in many states, including Florida, Georgia, Alabama, Virginia and the Carolinas. Moves more than 100 million gallons of fuel daily. The pipeline connects directly to major airports and tank farms along the system. The Largest tank farm is in Greensboro, North Carolina, where the two mainlines originating in Houston terminate. Deliveries to the Northeast originate from Greensboro. Airports connected include Atlanta, Charlotte, Greensboro, Raleigh-Durham, Dulles, and Baltimore-Washington. It's about 10 miles away from here, which we know because it leaked 2 million gallons of gas about 7 months before the pipeline was hacked in 2021. Discovered by two boys on ATVs, by smell.
Colonial Pipeline paid DarkSide hackers to get the decryption key, enabling the company's IT staff to regain control of its systems. US DoJ later recovered 63.7 bitcoin - worth about $2.3 million at the time - from the attackers.
How the hackers got in: A Colonial Pipeline employee - who was not publicly identified - likely used the same password for the VPN in another location. That password was somehow compromised as part of a different data breach. Password re-use is a human response, **don't fix the user.**
NIST 800 Adapted and re-used by private industry. Short version small business – NISTIR (Interagency Report) 7621, Revision 1 "Small Business Information Security: This 54-page publication is available free of charge from: https://doi.org/10.6028/NIST.IR.7621r1 and a ????
The Fundamentals 3-page "A Quick Start Guide," NIST SP 1271 available for free https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf

Now made this into the working Cybersecurity Framework update to 2.0 underway but not released
NIST simplified by Center for Internet Security, a non-profit organization
CIS simplification for size of business: Implementation Group 1. LINK
We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data.
The GCA Cybersecurity Toolkit for Small Business - Free and effective tools you can use today to take immediate action to reduce your cyber risk.
https://gcatoolkit.org/smallbusiness/standards/ UK Commonwealth.
“Coalition” paper, https://info.coalitioninc.com/download-2022-cyber-claims-report.html available for free download (gated for business email), probably the best example out there, clean and modern design. “Coalition is the world’s first Active Insurance company, providing a new model for risk management in the digital age. We were able to solve 46% of reported incidents at no cost to the policyholder.”
Small businesses are disproportionately impacted. As attacks become increasingly automated, it has become easier and more profitable for criminals to target small organizations.
Business Email Compromise with Financial Fraud is now the most common claim, although the financial impact of ransomware is still higher. BEC tends to be a quick in-and-out, more of a digital smash and grab.
A recent security firm survey found that more than half of businesses would reconsider partnerships with another organization lacking comprehensive cyber insurance.

End notes

----------=----------