

The Cyber Security Symposium Series

Is your business ready for the next cyber security threat?

December 17, 2020

Presented by

SYNOVUS[®]
the bank of here

and

 **CRI** CARR
RIGGS &
INGRAM
CPAs and Advisors

Today's Webinar: Housekeeping Items

- Today's webinar is being recorded.
- Attendees will be in listen mode with microphones automatically muted upon entry.
- For optimized viewing, we suggest that you change the screen view by hovering over the top right of speaker panels and choose Side by Side View.
- Questions are encouraged. Please enter them into the Chat feature.

Agenda

- Welcome & Introductions
- Challenges
- What you need to know
- What you can do
- What resources are available to help
- Q&A
- Closing Remarks

Host and Moderator



Kevin Gillen

Symposium Host

Market Executive SW FLA,
Synovus



Mary Harrington

Symposium Moderator

Treasury & Payment Solutions,
Synovus

Panelists



Enrique Fernandez

Director of Financial Crimes Unit,
Synovus



Serge Jorgensen

Founding Partner and Chief
Technology Officer, Sylint Group



Byron Shinn

CPA and Engagement Partner,
Carr Riggs & Ingram, CPA, LLC

424%

The percentage increase in cyber breaches last year

14%

Percentage rating their ability to mitigate cyber risks and attacks as highly effective.

52%

Data breaches caused by human error and system failure

\$383,365

Cost of cyber attacks caused by compromised employee passwords

3%

Cyber security budget should be at least 3% of a company's total spending.

Cybercrime To Cost The World \$10.5 Trillion Annually By 2025



Source: Cybersecurity Ventures
<https://www.thesslistore.com/blog/33-alarming-cybercrime-statistics-you-should-know/>

Challenges

I want to play a game with you. Let me explain the rules:
Your personal files are being del_

Maze Ransomware

Dear SYSTEM, your files have been encrypted by RSA-2048 and ChaCha algorithms
The only way to restore them is to buy decryptor

These algorithms are one of the strongest
You can read about them at wikipedia

If you understand the importance of situation you can restore all files by following instructions in
DECRYPT-FILES.txt file

You can decrypt 3 files for free as a proof of work
We know that this computer is a server in corporate network
So we will give you appropriate price for recovering



Time	Communications
07:45:16 PM	Welcome! We are ready to help you.
07:47:27 PM	OK - how can you help us?
07:52:44 PM	Hello, price for you is 10 000 000\$. This is the price for decryption keys and destruction of downloaded data from your network.
07:53:52 PM	This price can be splitted into separate payments. \$5M for decryptors and other \$5M later for destruction of downloaded data.
08:00:04 PM	can you provide us with samples of this date you have?
08:02:12 PM	Yes, please await I will ask data holder. Due to security reasons data is <u>held</u> only by one man will attach you files as soon as he sends this to u
09:36:15 PM	Ok, I will attach some proofs right now

https://[redacted]chat#info

You have **03:38:12**

Current price **114.39738836 BTC**
= 1,000,000 USD

After time ends **228.79477672 BTC**
= 2,000,000 USD

Bitcoin address [redacted]

* BTC will be recalculated in 4 hours with an actual rate.

INSTRUCTIONS | **CHAT SUPPORT** | ABOUT US

you keep mentioning GUPK...we are just [redacted] 15 minutes ago

It is not main. Main is we can publish data, financial data for example, and money will start to go missing and your company will be the source of that.
 Traveler could pay us \$3kk, but as result have paid to us double price, because they picked the wrong scenario. I recommend you not make same mistake. miser pays twice.
 Send to your committee we agree accept \$2kk
 6 minutes ago

Price updated to 2,000,000.
 4 minutes ago

Type your question here

Browse files for attach (maximum 3 files, less than 10MB) **SEND**

Crytek

Published: 100%

Crytek has been locked by Egregor

 ransomware

Visited: 15409

[Read more -->](#)

Ubisoft

Published: 50%

Ubisoft has been compromised by Egregor. We have sources of new Watch Dogs: Legion. Now we add TORRENT file for download.

 ransomware

Visited: 17424

[Read more -->](#)

Barnes & Noble B

Barnes & Noble Books

 ransomware

Visited: 10539

Ubisoft

 **TORRENT file**

Now we upload game Watch Dogs: Legion, engine and maintenance tools for this engine and game. Password for archive: !160j=3\$*dC2c3,bFv5k

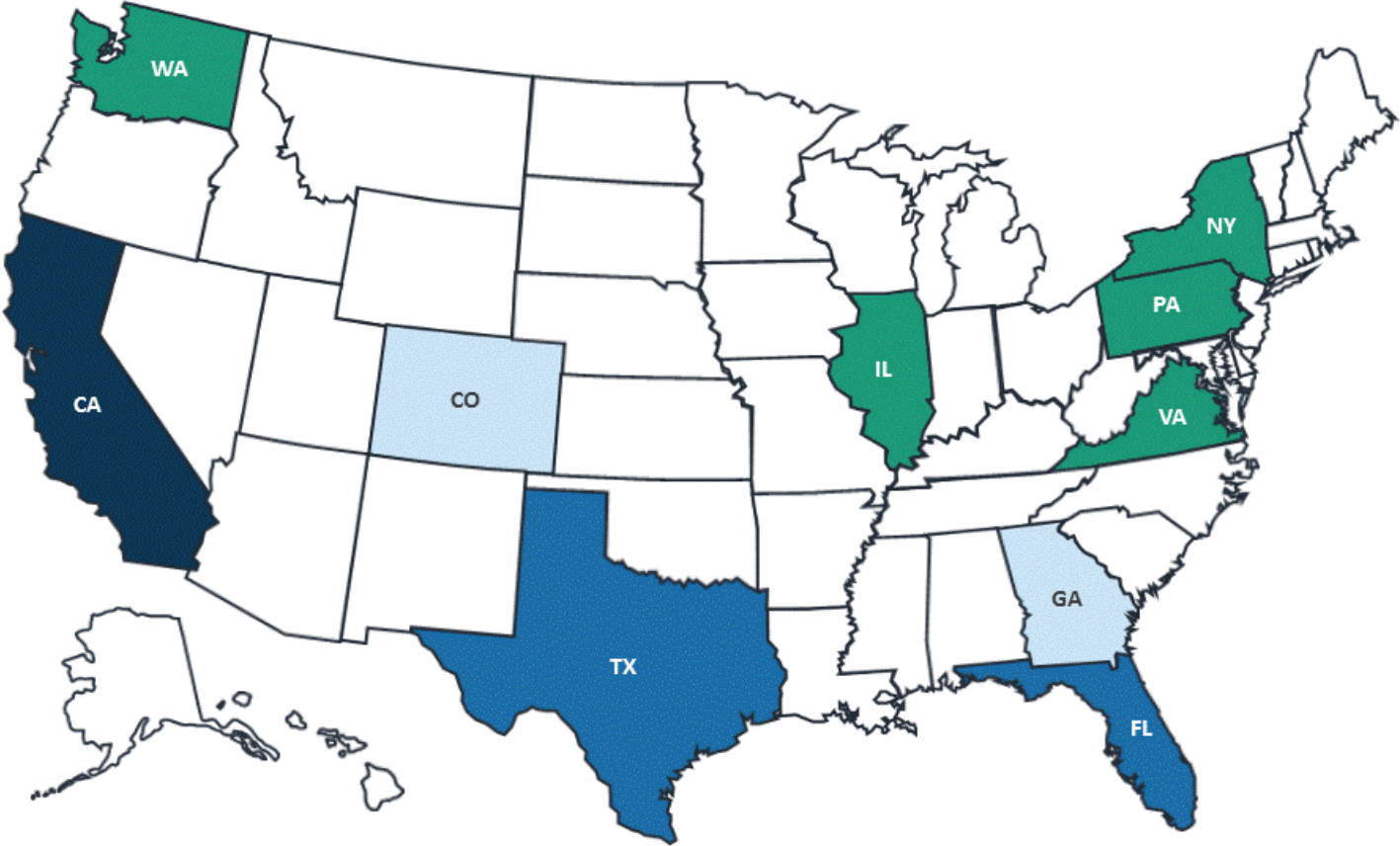
 **URL:** <https://www.ubisoft.com/>

 **Address:**

28, rue Armand Carrel,

93100 Montreuil-sous-Bois, France

Top 10 States by number of Victims



30,000+ 20,000 – 29,999 10,000 – 19,999 4,000 – 9,999

Challenges

- **76% of small businesses experienced a cyber attack in the last 12 months**
- **Risks lie both inside & outside your companies**
 - 69% of breaches were perpetrated by outsiders
 - 34% involved internal parties
 - 2% involved partners
- **There are many different tactics to defend against**
 - 52% of breaches caused by human error & system failures
 - 33% included social attacks & social engineering
 - 30% caused by phishing
 - 28% involved malware (delivered via email in 94% of cases)
 - 27% driven by stolen credentials
 - 15% included misuse of privileges by insiders

What you need to know

- **Cybersecurity represents a major risk to every company**, whether you're a target of a ransomware attack, theft of intellectual property, exposure of customer information, financial crimes, every company is at risk
- **Cyber isn't just the IT or Information Security area's responsibility** – you need to create an awareness and a culture where everyone has a stake in cybersecurity
- **Understand what your most valuable assets are** – your “crown jewels”, and what the risks are to their security. For example, how would you know if confidential data left your company?
- **Cyber risk** - What are your greatest cyber risks, why are they considered your greatest risks, what are you doing to manage them? What are the trends in your industry, region, etc.? How are you managing third-party risk? What is company's potential financial loss from a cyber event.
- **Threats** - Do you understand who our likely adversaries are and what they are most likely to attack? How do you gather threat intelligence?
- **What are your breach detection and response capabilities?** Are you practicing what to do in the event of a breach or security incident?
- **Program Maturity** - **How does your security program compare to industry peers?** What are your biggest cybersecurity gaps and what are we doing to mitigate them?
- **Security investments (people, \$)** - **Are you spending more or less than your peers?** How effective is your security spending? How is budget allocated among prevention, detection, and mitigation?
- **Third-party security assessments** – have you had an Independent risk assessment of your security program?
 - 3rd party security ratings, penetration tests, audit or regulatory assessments

How do they get in?



Everything's Secure



Or convenient?





Phishing Example

FILE MESSAGE McAfee E-mail Scan


Ignore Delete Reply Reply All Forward Meeting IM More Move OneNote Actions Mark Unread Categorize Tags Follow Up Translate Find Related Select Zoom Report Phishing PhishMe

Wed 1/10/2018 10:53 AM


 Drop~box <mchampion@cheetah.com>
[External] - Scanned Document - (Review & Sign)

To 

Use caution with attachments or links.

 **Dropbox**

You just received (1) document from James



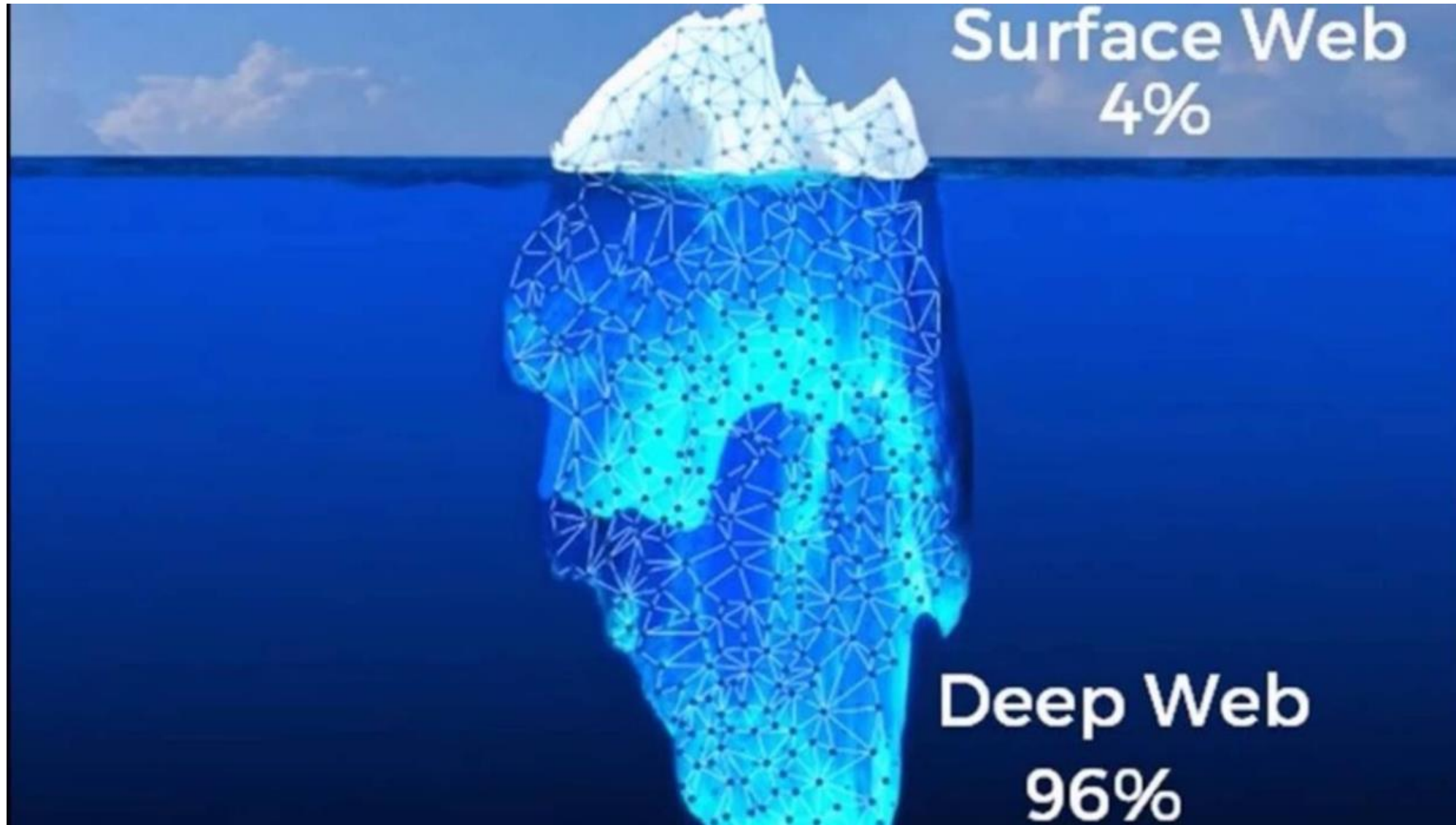
<https://imaject.info/xfileinc/1>
Click to follow link

Please ([Preview or Download](#)) here

Regard,
Dropbox


- Protect personal and financial information online
- Use security software for computers and mobile phones
- Don't fall for Phishing scams
- Use strong and *unique* passwords
- Use Multi-Factor Authentication whenever possible (MFA)
- Shop only secure websites (https in web address)
- Avoid shopping on public (“free”) Wi-Fi
- Get an Identification Protection PIN from Treasury (available for all)
- Send data encrypted AND double check the recipient address

Deep / Dark Web



Dark Web

pspherexxxxxxxxxx.onion/index.php?file=Classical DBs



PROJECT SPHERE

Welcome to the Sphere files

News adds of the Week

Files :

- Classical DBs/U.S. Government mails.txt
- Classical DBs/New York City Emails-Leak.txt
- Books/Easy Cash Version 1.1 Brand New.pdf

Folders :

- Classical DBs/Password Lists for bruteforce

Officials Links :

- Project Sphere >> [psphere36sxsxv2vr.onion](#)
- Project Sphere Upload >> [psupload34nbfv6q.onion](#)

Classical DBs

Search for classical Data Bases from different Websites, Server Infrastructures

section	size	status
Go back	48.61 GB	GO back
Iron March DB	979.45 MB	ONLINE
Panama Papers Leak	58.63 MB	ONLINE
Password Lists for bruteforce	459.74 MB	ONLINE
11k-hacked-hackforums-accounts.txt	461.51 KB	ONLINE
15k USA mails.txt	490.57 KB	ONLINE
ClientsDB(elfassiscoopblog).pdf	1.99 MB	ONLINE
combo.txt	74.03 KB	ONLINE
Combos_5.txt	9.01 MB	ONLINE
DB.marc-uzan-expertise-philatelie(SG).txt	178.86 KB	ONLINE
MAILSDB.txt	524.02 KB	ONLINE
tinsite.com_mails6passwords.txt	85.42 MB	ONLINE
les (rhone-alpes.culture.gouv.fr).txt	8.55 KB	ONLINE
ty_Emails-Leak.txt	387 bytes	ONLINE
e.txt	77.03 KB	ONLINE

ssnxxxxx.onion/nova-search.php#

SSN Search Super Search by State Nova Search Used Data MMN Search Stuff Rules

Balance: [] []

FIXED NOVA SEARCH ***** SSN24.CC - RESERVE DOMAIN SAVE IT !!! !! cc-stock.hk - NEW CC SHOP ...!!

Arkansas William Clinton Search

Status: OK (11) Purchased Only Search in history History

Name	Address	DLN / Phone / Email	SSN	DOB	Buy
William C Clinton	6604 Navaj North Little Rock, AR 72116 North Litt North Little Rock, AR 72116 Trl Navajo North Little Rock, AR 72116	Phone: 50122...		1962-10-...	Buy
William Clinton	1828 Hogan Sherwood, AR 721206536 25 Campden Sherwood, AR 721206536 Conway Ar Sherwood, AR 721206536	Phone: 50134...		1993-12-...	Buy
William Clinton	1828 Hogan Conway, AR 720347467 25 Campden Conway, AR 720347467 Conway Ar Conway, AR 720347467	Phone: 50134...		1993-12-...	Buy
William Clinton	813 Greend North Little Rock, AR 721174529 901 Greend North Little Rock, AR 721174529	Phone: 50141...		1976-06-...	Buy
William Clinton	813 Greend North Little Rock, AR 721174502 901 Greend North Little Rock, AR 721174502	Phone: 50141...		1976-06-...	Buy
William Clinton	3990 Darwi Jacksonville, AR 720769207 8 Cherryri Jacksonville, AR 720769207 Ave Darwin Jacksonville, AR 720769207 Jacksonvil Jacksonville, AR 720769207 San Diego Jacksonville, AR 720769207	Phone: 50151...		1987-05-...	Buy
William Clinton	6604 Navaj North Little Rock, AR 721165320 North Litt North Little Rock, AR 721165320 Trl Navajo North Little Rock, AR 721165320	Phone: 50122...		1962-10-...	Buy
William Clinton	6604 Navaj North Little Rock, AR 721165320 North Litt North Little Rock, AR 721165320 Trl Navajo North Little Rock, AR 721165320	Phone: 50122...		1962-10-...	Buy

Dark Web

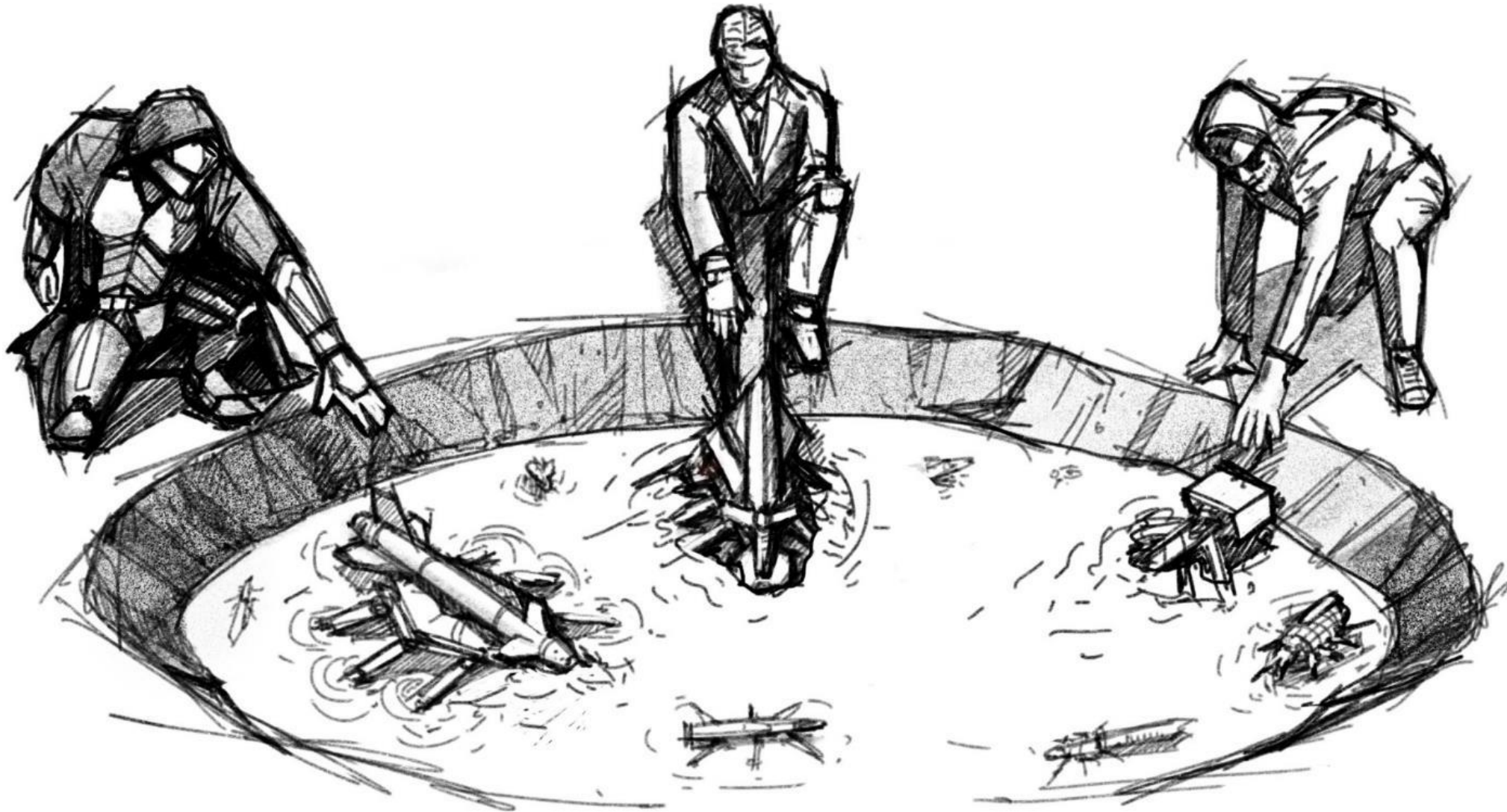
The screenshot shows a browser window with the address bar containing 'magbooooo.onion/sys'. The page header features a profile picture of a purple cat, the name 'Bo Store', and the tagline 'The best thing on the dark side.' To the right of the header are several utility icons: a megaphone, a gear, a microphone, a location pin, a question mark, and a power button.

The main content area is split into two columns. The left column displays a timestamp 'Thu, 10 Dec 2020 23:51:43 +0300 BTC \$18382' and a redacted area. Below this are three statistics: '0 purchases', '0 sales', and '0 activity'. A 'Reviews' section shows five vertical bars, a 'Rating' of '0.00' in a green box, and a 'Total' of '\$ 0'. At the bottom of this column, a red banner shows a balance of '\$ 0.00 + \$ 0.00' and '฿ 0.000000 + ฿ 0.000000' with a sad face icon.

The right column contains a list of items or ads:

- Ad from pageranks:** I buy DA 30+ clean shells in bulk. BTC always ready. Looking for long term providers. PM me list or Telegram @mark5934 for immediate deal. Sellers: contact me before listing. ;)
- Ad from xgrx:** Sell a method of extracting clean shells and adminpanels with good DA + Bonuses. <https://shoppy.gg/product/njCOWP>
- System News:** Security Levels *statistic*. I ask sellers to take it into account.
- Ad from moneyfeel:** Selling SMTP accessess for spam (not shells). Many of them have IMAP/POP3 access. Price: <https://pastebin.com/raw/Syt4Zj9F> | Jabber: moneyfeel@thesecure.biz / Telegram: @mofeel

Dark Web



Albert "segvec" Gonzalez

- Born in 1981
- An American Computer Hacker & Computer Criminal
- ShadowCrew - screen name "CumbaJohnny"

Trafficked stolen credit and ATM card numbers

- Hacked the databases of TJX Companies - 45.6 million credit and debit card numbers
- Heartland Payment Systems, Citibank
- Hacked computer systems of the government of India
- Arrested on May 7, 2008 - was sentenced to prison for 20 years



Jonathan James

- Born on December 12, 1983, United States of America
- c0mrade
- Hacked software of NASA
- Hacked software of DOD - Between August 23, 1999, and October 27, 1999
- Arrested and sentenced to six months
- Died on May 18, 2008



Ross Ulbricht

- Born in 1984
- An American Cyber Criminal
- Eagle Scout, BS in Physics & Masters in Materials Science
- Pseudonym “Dread Pirate Roberts”
- Created darknet market website Silk Road in 2011
- “I am creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force”
- Site was designed to use Tor for anonymity and bitcoin for currency
- Arrested in 2015 & sentenced to life in prison





WANTED BY THE FBI

CONSPIRACY TO COMMIT COMPUTER FRAUD; CONSPIRACY TO COMMIT WIRE FRAUD; WIRE FRAUD; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

GRU HACKING TO UNDERMINE ANTI-DOPING EFFORTS



Dmitry Sergeyevich
Badin



Artem Andreyevich
Malyshev



Alexey Valerevich Minn



Aleksei Sergeyevich
Morenets



Evgenii Mikhaylovich
Karakhanov



Oleg Mikhaylovich
Koshnikov



Ivan Sergeyevich
Yarmakov

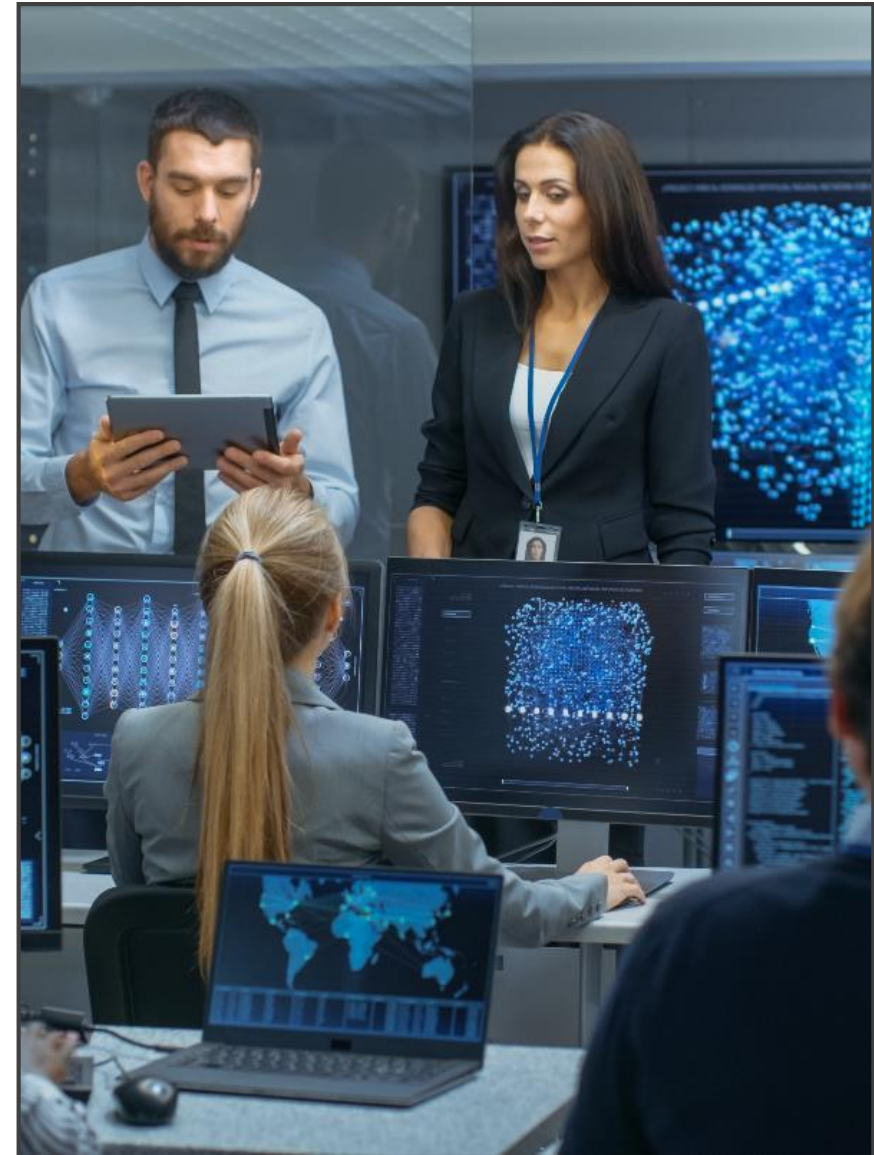
WANTED BY THE FBI





Be Prepared

- Review current company policies & procedures including regular updates as your business grows and adapts.
- Review with legal counsel for protection
- Review insurance *and its limitations*
- Discuss areas of improvements with IT
- Consider leveraging a third party to assess current security posture and provide recommendations



Top 30 Passwords

- | | | |
|---------------|---------------|--------------|
| 1. 12345 | 13.Aa123456. | 25.111111 |
| 2. 123456 | 14.iloveyou | 26.ashley |
| 3. 123456789 | 15.1234 | 27.00000 |
| 4. test1 | 16.abc123 | 28.000000 |
| 5. password | 17.111111 | 29.password1 |
| 6. 12345678 | 18.123123 | 30.monkey |
| 7. zinch | 19.dubsmash | |
| 8. g_czechout | 20.test | |
| 9. asdf | 21.princess | |
| 10.qwerty | 22.qwertyuiop | |
| 11.1234567890 | 23.sunshine | |
| 12.1234567 | 24.BvtTest123 | |

Risk Assessments & Response Plans

- Engage in an Overall Risk Assessment
 - Identify and prioritize areas to address immediately
 - Identify User Access Routes & Methods
- Cyber requirements for Department of Defense Prime and Subcontractors are **no longer voluntary**
- Review or Develop
 - Communication and recovery plans
 - System Security Plan (SSP) with verifiable and auditable requirements
 - Written Incident Response Plan (WISP)

Actions to take now

- Conduct ongoing training for employees on security issues and hold them accountable to follow *all* processes and procedures
- Don't use email for financial transactions without verification
- Manage user IDs & passwords and use multifactor authentication wherever possible
- Keep computers and other devices updated with latest releases & patches
- Create (and test) backups for all important information
- Pay attention to all devices connected to your network, not just computers (“Internet of Things”)
- Secure your wireless network and don't allow guest access to your company network
- Bring in outside expertise to assess your risk and test your security
- Develop and document a cybersecurity plan – and test it

Key Takeaways

- **Security is everyone's responsibility**
 - Train your employees and hold them accountable
- **Don't rely on emails for financial transactions**
 - Verify requests and have sound business processes
- **Backup your critical information regularly**
 - *Test* your backup to assure it is functioning correctly
- **Understand your contract when you use 3rd party services**
 - Be clear on scope, responsibilities, and service levels
- **Have an Incident Response Plan in place**
 - Know how to respond and have contacts established

What resources are available to help

Take advantage of the resources and information that is available

- FBI Internet Crime Complaint Center (IC3)
 - <https://www.ic3.gov/default.aspx>
- Federal Trade Commission
 - <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>
- U.S. Small Business Administration (SBA)
 - <https://www.sba.gov/managing-business/cybersecurity>
- U.S. Department of Homeland Security – U.S. Computer Emergency Readiness Team (US-CERT)
 - <https://www.us-cert.gov/ccubedvp/smb>
- Synovus
 - Safety and Security - <https://www.synovus.com/contact-us/safety-and-security/>
 - Personal Resource Center - <https://www.synovus.com/personal/resource-center/#security>

Q&A

Enrique A. Fernandez

Director of Financial Crimes Unit, Synovus

enriquefernandez@synovus.com

Serge Jorgensen

CTO, Sylint Group

sjorgensen@syLint.com

Byron Shinn

Partner, Carr Riggs & Ingram

bshinn@cricpa.com

Mary Harrington

FVP Treasury & Payment, Synovus

MaryHarrington@synovus.com

Thank you for attending

A brief survey will be sent to you from Events@Synovus.com.

Thank you in advance for your time and feedback.



and



CRI CARR
RIGGS &
INGRAM
CPAs and Advisors

Appendix

SYNOVUS[®]
the bank of here

and



CRI CARR
RIGGS &
INGRAM
CPAs and Advisors



Kevin Gillen

Symposium Host

Market Executive SW FLA,
Synovus

Kevin has over 40 years' experience in the banking industry. He is Market Executive for Synovus Bank in the Florida Division comprised of 72 full service commercial branches. Kevin supports the commercial, business banking and retail sales, marketing and business development strategy and new hire on boarding for the commercial and business bankers in Florida.

He was previously Director of Supply Chain Strategy for Private Eyes Inc. and 4506 Transcripts; two companies, same ownership. Private Eyes is a Global Employment Background & Drug Screening Company. 4506 Transcripts.com is a large IRS bulk approved vendor for tax transcripts integrated with Fannie Mae, Ellie Mae.

Kevin was Executive Vice President, Retail Lending Director for TD Bank which included a \$36Bn residential mortgage and home equity portfolio. He was responsible for product development, pricing, secondary market sales, risk, US sales.

Prior to this role, Kevin was, EVP- Head of Retail Strategy and Solutions for TD Bank. He was responsible for US Retail Sales, Operations, Distribution, Risk, ATM and the Contact Centers. Total operating budget was \$1.6Bn with 14,000 employees.

Previously, Kevin was the Regional President for TD Bank's Florida market; overseeing retail, consumer, commercial & middle market lending, government banking, and cash management. His former roles include Market President for Metro D.C., New York, New Jersey and Pennsylvania.

Prior to joining TD Bank, he was a member of Summit Bank's senior leadership team for 19 years and was the Regional President for the bank's New Jersey business.

He was appointed by former Florida Governor Scott to the Enterprise Florida Board. He was on the board for The Broward Workshop and the Florida Bankers Association.

He was a member of SHRM and the Sarasota / Manatee SHRA Chapter; College Relations Chair, board member for Family Success Institute and a pre-IPO mortgage service firm. He is Chair for Jesus Father of the Poor Clinic – Haiti. He is an advisory board member for the business and accountancy school at State College of Florida.

He served in numerous New Jersey, Virginia and Washington DC based community organizations as board and chair roles.

Kevin graduated Lycoming College - BA in Business Administration, Sociology & Anthropology.



Mary Harrington

Symposium Moderator

Treasury & Payment Solutions

Synovus

Mary is a Senior Technical Consultant with the Treasury & Payment Solutions team at Synovus Bank. She has over 30 years of Banking, Payments Technology and Treasury Management experience including Sales Management, Product Development, Training, and Payables/Receivables solution consulting. Her passion is helping clients by sharing insights on the latest fraud trends and best practices in mitigation strategies. She works closely with the Synovus Fraud and Financial Crimes Unit teams to stay abreast of the critical issues impacting both the Bank and our clients. She has been a frequent Cybersecurity speaker in Florida for events including the Florida Government Finance Officers Association (FGFOA), Florida Bar Association and Association for Financial Professionals (AFP). Mary has a B.S. in Finance from Miami University and is a Certified Treasury Professional.



Enrique Fernandez

Director of Financial Crimes Unit,
Synovus

Enrique oversees the Financial Crimes Unit at Synovus. He joined Synovus after the FCB acquisition in the 2019 as an effective domestic and international banking business professional with more than 20 years managing corporate security and risk management, inclusive of banking fraud investigations, cyber fraud & intrusions and physical security. Prior to joining Synovus he managed the investigation's unit at BankUnited for over 10 years. He started his banking career as young associate back in 1995 with First Union National Bank, joining the Fraud Investigations team in 1999. Enrique is an active member of United States Secret Service Electronic Crimes Task Force and president of Financial Institution Security Association.



Serge Jorgensen

Founding Partner and Chief
Technology Officer, Sylint Group

Serge Jorgensen is a founding partner and Chief Technology Officer in the Sylint Group, and provides technical development and guidance in the areas of Computer Security, Counter CyberWarfare, System Design and Incident Response. Mr. Jorgensen is a patented inventor in engineering and security-related fields, has held various security clearances and works closely with the FBI, DHS and others in tasking, analyzing and managing Information Security needs to safeguard critical infrastructure, manufacturing and other operations.

Sylint

Sylint provides leading edge expert services in Cyber Security, Digital Data Forensics, and eDiscovery. Formed in 1998, our firm has developed a national reputation as a leader in its field, and works internationally with Fortune 50 organizations to small firms and municipalities. Sylint is one of the few Payment Card Forensic Investigation and NSA-accredited Incident Response companies, with experience from National Intelligence Agencies, Department of Defense, law enforcement, and corporate entities used to provide comprehensive cyber security and investigative services. Services include detection and remediation of corporate espionage, fraud identification, cyber security posture review, and regulatory compliance.



Byron Shinn

CPA and Engagement Partner,
Carr Riggs & Ingram, CPA, LLC

Experience

Mr. Shinn is a partner in the Bradenton/Sarasota Region with over 38 years of public accounting experience. Byron leads and provides professional and responsive services in the areas of auditing, internal audits accounting, taxation and business consulting. Byron started Shinn & Co. in 1993 and merged into CRI in 2018. Prior to starting Shinn & Co, Byron worked for both local CPA firms as well as Arthur Andersen. Byron is very active with the Florida Board of Accountancy, having held positions as a member of the Probable Cause Panel (15 years) and Chair of the Board. Byron is on the Board of Trustees for the University of South Florida and a board member of the Sarasota Economic Development Council. Prior involvement has included past Chairman of the Florida Board of Accountancy, President of the Manatee Chamber, Past President of Kiwanis Club of Bradenton, Past Board Member of United Way of Manatee County, just to name a few.

Education, Licenses & Certifications

- B.A. University of South Florida, June 1979, Major in Accounting
- A.A. Manatee Junior College, June 1977
- CPA, State of Florida

Professional Affiliations and Organizations

- * American Institute of Certified Public Accountants (AICPA)
- * AICPA – Tax Practice & Procedures Committee
- * Florida Institute of Certified Public Accountants (FICPA)
- * Institute of Internal Auditors member
- * Bradenton Blue Foundation, Board member
- * EDC Sarasota, Board member
- * EDC Bradenton Area EDC
- * Florida Maritime Museum, Treasurer
- * University of South Florida, Trustee
- * Appointed to Florida Cybersecurity Task Force