

SECURITY & RISK 2019

Hackers vs. Executives

*Josh Zelonis, Principal Analyst
September 13, 2019*

FORRESTER **EVENTS**



1

SECURITY & RISK 2019

#FORRSecurity

James Webster

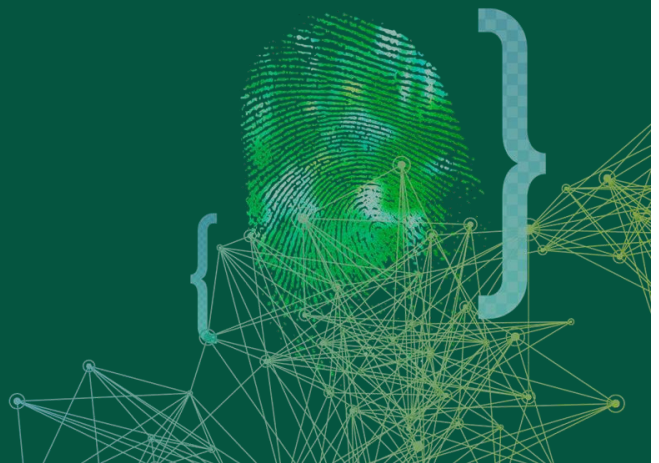
Vice President of Infrastructure and Operations/CISO,
ManTech

Olivia Rose

CISO,
Mailchimp

Josh Zelonis

Principal Analyst
@josh_zelonis



2

The Panel



Olivia Rose

CISO, Mailchimp



James Webster

Vice President of
Infrastructure and
Operations/CISO,
ManTech



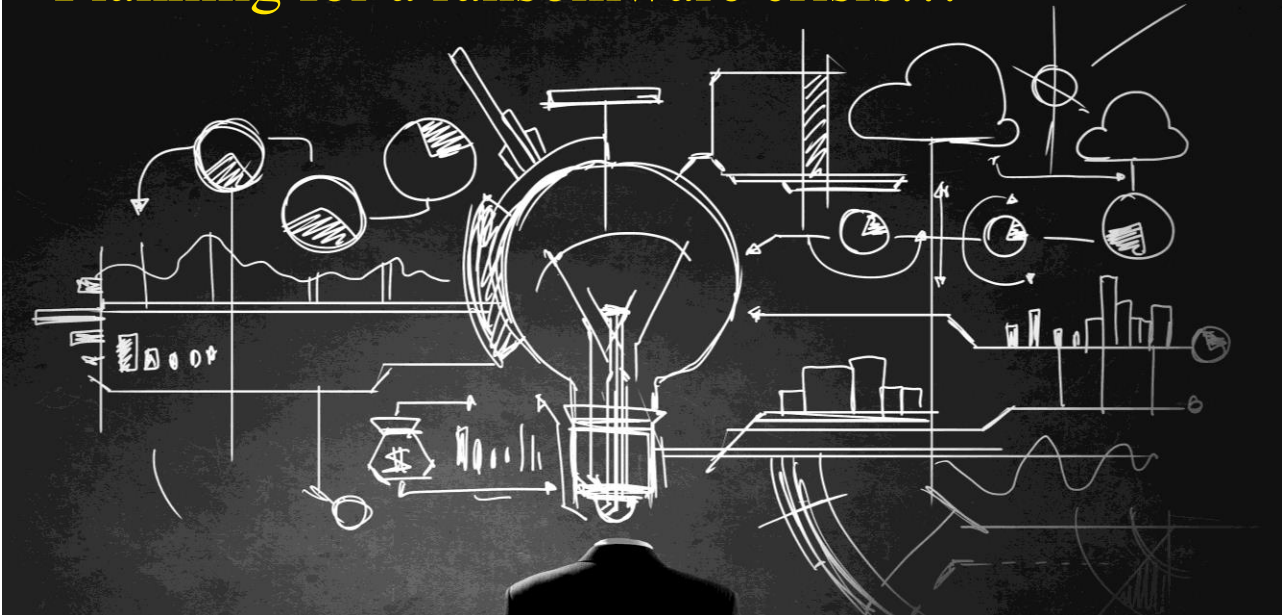
Russ Cohen

Vice President,
Cyber Services,
Chubb

© 2019 Forrester. Reproduction Prohibited.

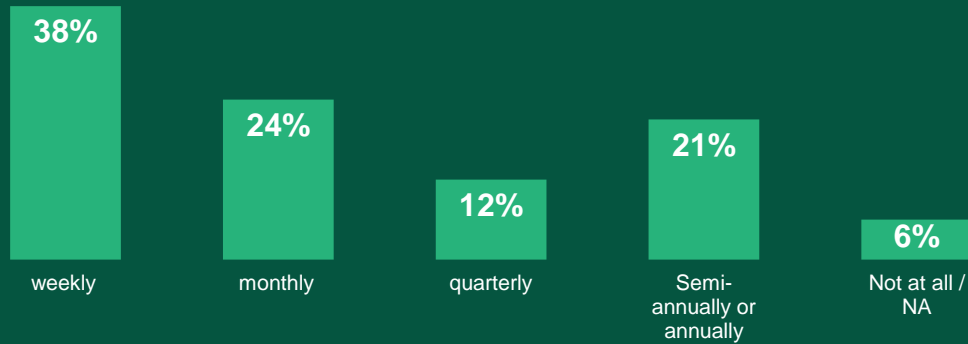
3

Planning for a ransomware crisis...



4

Are you Confident In Your Ability To Restore Backups?



Base: 34 information professionals who said that business continuity and/or disaster recovery, enterprise architecture, information security or infrastructure and operations best described the organizational group to which they belonged.
© 2019 Forrester. Reproduction Prohibited.

5

Your network has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - **gl74809ja-Decryptor**

You can do it right now. Follow the instructions below. But remember that you do not have much time

gl74809ja-Decryptor price
the price is for all PCs of your infected network

You have **6 days, 23:59:00**

Current price **2.08192261 BTC**
≈ 20,000 USD

* If you do not pay on time, the price will be doubled

6

Let's Call In The Air Support



Tim Parisi

Director, Incident
Response Services,
CrowdStrike



Tom Hofmann

VP of Intelligence,
Flashpoint

© 2019 Forrester. Reproduction Prohibited.

7

Home PayPal Banks Shopp CC Services												
Home / Dedicate (10815)												
<input type="text" value="Search"/>												
OS / Lang	Ram	CPU / Core / Bits	AV	Browse	Not Used	UP / DL	Root	NAT	Location	Checked	Port	Seller
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: United States State: California City: Los Angeles Zip: 75007	11-05-2018	3389	Fantasy
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: Singapore State: Central Singapore Community Development Council City: Singapore Zip: 22042	11-05-2018	3389	iDed
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: United States State: Florida City: Boca Raton Zip: N/A	11-05-2018	3389	Fantasy
Windows Server 2012 [English]	4.00 GB	Intel(R) Xeon(R) CPU E5... CPU Core: 2 Bits OS: 64	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 9.84 Mbit/s DL: 14.05 Mbit/s	yes	no	Country: United States State: Arizona City: Scottsdale Zip: 85260	11-05-2018	3389	iDed
Windows 7 [English]	2.00 GB	Virtual CPU a7769a638... CPU Core: 1 Bits OS: 32	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 74.32 Mbit/s DL: 12.65 Mbit/s	no	no	Country: Hong Kong State: N/A City: N/A Zip: N/A	11-05-2018	3389	iDed
Windows Server 2012 [English]	1.75 GB	AMD Opteron(tm) Proce... CPU Core: 1 Bits OS: 64	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 10.86 Mbit/s DL: 13.29 Mbit/s	no	yes	Country: United States State: Texas City: San Antonio Zip: 94948	11-05-2018	3389	iDed

8



9

```

readme.txt - Notepad
File Edit Format View Help
----- Welcome. Again. -----

[+] Whats Happen? [+] Misspelling of extension
Your files are encrypted, and currently unavailable. You can check it: all files on you computer
has expansion [REDACTED].
By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]
Its just a business. We absolutely do not care about you and your deals, except getting benefits.
If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our
interests.
To check the ability of returning files, You should go to our website. There you can decrypt one
file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your
time and data, cause just we have the private key. In practise - time is much more valuable than
money.

[+] How to get access on website? [+]
You have two ways:

1) [Recommended] Using a TOR browser!
a) Download and install TOR browser from this site: https://torproject.org/
b) Open our website:
http://[REDACTED]:f56nf6aq2nmyoyd.onion/[REDACTED]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For
this:
a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
b) Open our secondary website: http://decryptor.top/[REDACTED]

Warning: secondary website can be blocked, thats why first variant much better and more
available.

```

10



11

Thank You.

Josh Zelonis

jzelonis@forrester.com

[@josh_zelonis](#)

© 2019 Forrester. Reproduction Prohibited.

12