KnowBe4
Human error. Conquered.

What Security Experts *Worry* About For 2019

The top threats that will impact your organization, and the world, in 2019 and beyond

Stu Sjouwerman
Founder and CEO
KnowBe4, Inc.

Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.

About Us:

Stu Sjouwerman

Founder and CEO, KnowBe4, Inc.

- Serial Entrepreneur, this is my fifth startup.
- Founded KnowBe4 after building an antivirus platform from scratch (VIPRE)
- Over 600 employees in Tampa Bay, FL as well as 5 office locations across the world
- Decades-long experience in creating system admin and security tools for IT professionals

Perry Carpenter

Chief Evangelist & Strategy Officer

- MSIA, C|CISO
- Former Gartner Analyst leading research and advisory services to CISOs, Security Leaders, and security vendors around the world
- Led security initiatives at Fidelity Information Services, Alltel Telecommunications, and Wal-Mart Stores
- Lover of all things:
  - Security
  - Psychology
  - Behavioral Economics
  - Communication Theory
  - Magic, misdirection, and influence

About KnowBe4

- The world's most popular integrated new-school Security Awareness Training and Simulated Phishing platform, over 22,000+ customers worldwide
- Founded in 2010
- Recognized as a Leader in the Gartner Magic Quadrant for Computer-Based Training (CBT)
- Our mission is to train your employees to make smarter security decisions so you can create a human firewall as an effective last line of defense when all security software fails…

Which it will

Agenda

- 2018 Review
- 2019 Threats
- What you can do now

Agenda

- 2018 Review
- 2019 Threats
- What you can do now

Prevailing 2018 Trends & Observations – Part 1

- Antivirus died in 2018. IT Pros are moving to (free) Win10 Defender in droves.
- GDPR came into being and the ramifications are not yet fully known.
- Trojans jumped to the top of the malware list. The most dangerous sign is the unfolding merger of trojans and phishing emails that amplifies the spreading of the malware
- Ransomware declined in volume but got more focused and highly damaging
- Crypto-ransom infections started out in high volume but declined over the year because of the continuing e-currency crash

Prevailing 2018 Trends & Observations

- The combination of Spam and phishing have kept at the same percentage levels, however phishing slice of the pie increased, and has gotten significantly more sophisticated
- CEO Fraud—aka Business Email Compromise—has taken flight in 2018 and shows no signs of abating. On the contrary, the bad guys are cooking up new schemes at a dizzying rate

And many organizations *still* did not adequately prepare their *last line of defense*…

Agenda

- 2018 Review
- 2019 Threats
- What you can do now


Evolution of
Computing =
Threats Evolved

All advancements come with unintended consequences

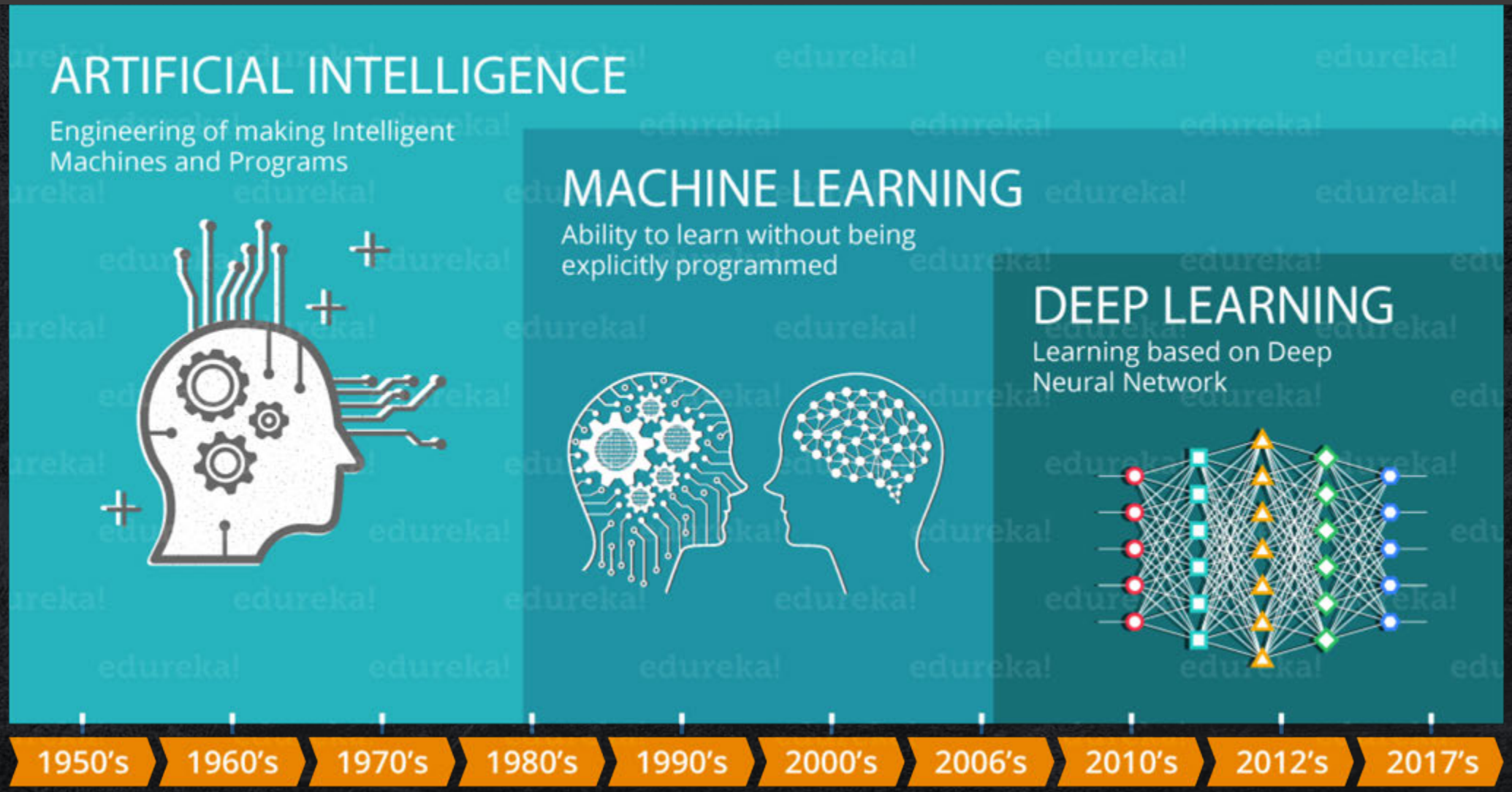
Understanding the fundamentals

Artificial Intelligence:

"the science and engineering of making intelligent machines, especially intelligent computer programs"

-- 1955, John McCarthy, the Father of AI

Understanding basic terms



Source: http://houseofbots.com/news-detail/2754-1-a-take-on-deep-learning

Aggregation

- Big Data
- Social Media
- Breach Info
- Credit reporting & background info data

Impersonation

- Google Duplex
- Adobe VoCo
- Deepfake
- Lyrebird
- Chatbots
- Etc…

MOTHERBOARD

DEEPFAKES

People Are Using AI to Create Fake Porn of Their Friends and Classmates

Facial recognition apps make it super easy to match anyone's face with a porn performer's body.

GIZMODO VIDEO SPLOID PALEOFUTURE IO9 SCIENCE REVIEW FIELD GUIDE DESIGN

Deepfake Videos Are Getting Impossibly Good

George Dvorsky
Tuesday 1:05pm • Filed to: FAKE NEWS

Reference Our Result

Left: Real footage of Vladimir Putin. Right: Simulated video using new Deep Video Portraits technology.
GIF: H. Kim et al., 2018/Gizmodo

Lyrebird AI Mimics Celebrity Voices
Fanatical Futurist
YouTube - Nov 13, 2017

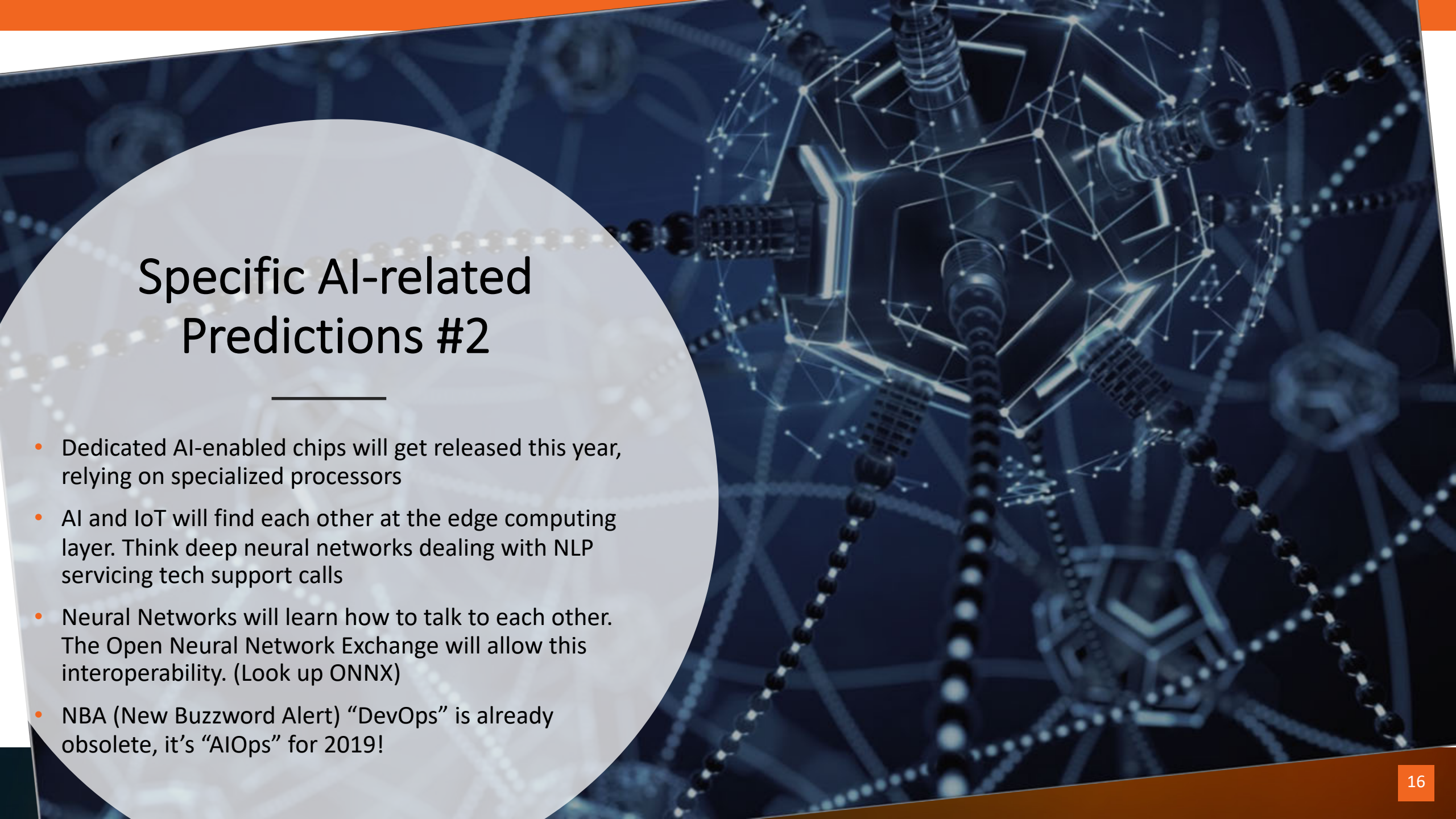
Fake Obama created using AI tool to make phoney speeches
World Live
YouTube - Jul 17, 2017

Lyrebird Says Trust No One
TWiT Netcast Network
YouTube - Apr 26, 2017

Source Sequence | Our Reenactment (Full Head) | Averbuch-Elor et al. 2017

Specific AI-related Predictions #1

- AI-based attacks will increase attacker capabilities and scale. Hearing about AI-driven attacks will become the new norm.
- There will be more targeted AI-driven fake news intended to cause disruption and societal chaos.
- 2019 will see the first AI-driven phishing attack at scale (20m+) – which will consist of highly personalized laser phishing, with an all-time high click-through rate of more than 50%.
- Skynet will become self-aware ...and we for one welcome our new electronic overlords. (*OK, this isn't an official prediction, but we feel better knowing that our new overlords have read it*).



Specific AI-related Predictions #2

- Dedicated AI-enabled chips will get released this year, relying on specialized processors
- AI and IoT will find each other at the edge computing layer. Think deep neural networks dealing with NLP servicing tech support calls
- Neural Networks will learn how to talk to each other. The Open Neural Network Exchange will allow this interoperability. (Look up ONNX)
- NBA (New Buzzword Alert) “DevOps” is already obsolete, it’s “AIOps” for 2019!

Quantum Crypto Becomes a Nearer-Term Worry

The day when quantum computers outperform traditional, binary, computers will happen in 2019. The incredible advancements made in quantum computing on a routine basis are going to make 2019 the year of the ultimate digital crossing-the-rubicon. This may or may not also be coupled with enough quantum accuracy to make anything traditional public key crypto (e.g. RSA, Diffie-Hellman, etc.) protects suddenly not protected. A decade later the NSA will tell us they had done this years before the public knew about it.

Photo of IBM Q: https://www.enterprisetimes.co.uk/2017/03/06/ibm-delivers-commercial-quantum-computing/


More Laws &
Regulations
Ahead

More Laws and Regulations Ahead

- A wave of huge GDPR fines will impact North American companies operating in Europe
- National Privacy Law will be created, and we will hate it
- 2019 will be the first year that legislation will be signed into law requiring *at least yearly* security awareness training combined with frequent social engineering tests.


It’s all
about the
data

Data-Level Attacks

- **Data exfiltration will become the new hot topic**
  - There is value in data, and immense amounts of data are being collected by both the private and public sectors. Attackers will not only continue to ransom data for recovery, but will also find creative ways to exfiltrate data then demand a ransom for its destruction, or keep silent about the fact that they exfiltrated the data in the first place.
  - As more and more executives are being held responsible for breaches, and as company valuation is impacted negatively, it is becoming more important for them to avoid this sort of disclosure. The bad guys know this and will exploit it.
- **Data Integrity Attacks**
  - On a related topic, several experts are predicting that data integrity attacks are going to be a big deal soon...where attackers, unknowingly to the victim, modify critical data so that the desired outcome is not reached. And the system owners or stakeholders can't rely on the system until they are able to restore the data to a known clean state.


Geo-Political
Turmoil

Algorithms Become the Next Cold War

- AI will increasingly be used to find and suggest new ways to exploit users and situations
- Algorithms are already ruling the world. The future of computer security and hacking are competing algorithms which simultaneously war against each other in a digital battle of good vs. evil. Taking advantage of the improvements in AI, humans will have less and less involvement in their security consoles. Basically, once set up they take over and do a better job defending networks and computers than those that have a more hands-on approach. The computer scientists who perfect these algorithms are the rock stars of 2019 and beyond. Being an “algo”, shorthand for algorithm engineer, will become one of the most sought after, sexiest jobs one can get.

Things Get Political… Again

- **Escalated Fake News**: Continued creation of fake news stories to drive division and behavior as 2020 US Presidential hopefuls declare their candidacies
- **Presidential Data Leak**. The US President's unwillingness to use more secure devices will lead to one of the most embarrassing political data leaks of all time.
- **Playing the Blame Game**: Nation-to-Nation false flag attacks
- **GRU Gone Wild**! The WannaCry damage will be nothing compared to new zero-day destructive malware that will be unleashed by the GRU on Ukraine but escape into the world at large and wreak havoc.

Ransomware, Pseudo Ransomware, and Sextortion

- More Ransomware and Pseudo-Ransomware: What works, stays. Expect to see more of both of these because they create immediate fear and situations that people need to react to. The feeling of loss or potential loss motivates people and can often bypass logic and reason. Also, more crypto mining in disguise
- More sextortion schemes that leverage past data breaches, current social network scraping, and more to create scary scenarios for those on the receiving end. In many ways, this is social engineering at a new devious low and recently got combined with GandCrab ransomware
- Ransomware attacks have been less prevalent in the news as the year has progressed, however, it doesn't mean they are stopping, they just aren't as newsworthy. Expect to see another ransomware attack, similar in size and scope as NotPetya and WannaCry, that will be different enough, have new enough capabilities, or cause enough damage to put ransomware back on the front page. The attackers have been working hard to find a new attack vector and got used to big paydays. They aren't going away any time soon

Wild-Ass Guesses

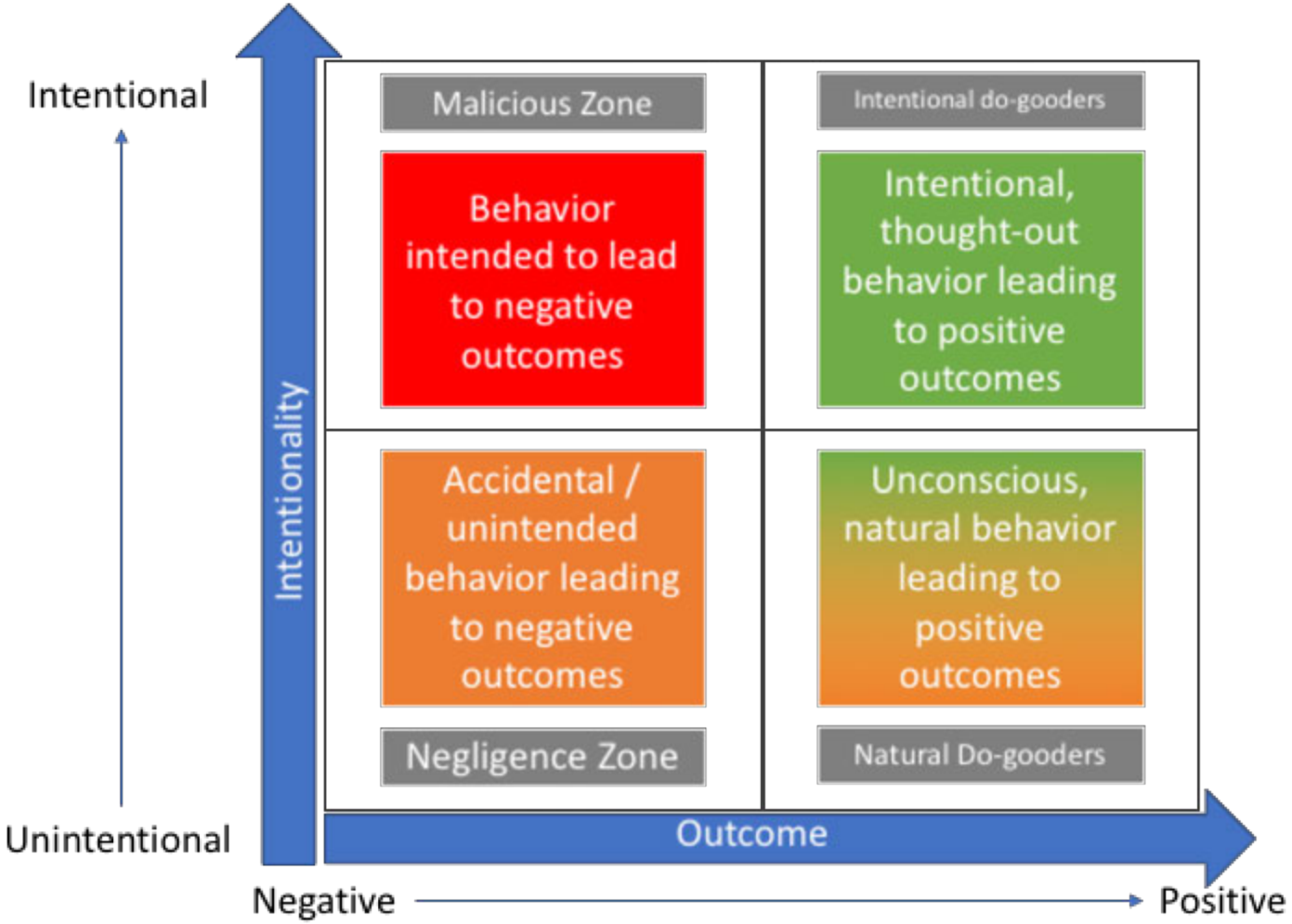
- A highly popular Chrome browser plug-in will be compromised and become the world's 1st 100M botnet
- A brand-new strain of malware will arrive in the wild - like CryptoLocker Ransomware in Sept 2013
- 2019, the year of the first billion-dollar cyberheist and a government having to step in as a back-stop
- Major AV engines will be completely circumvented by malware that has AI-driven evasive techniques
- China will test a combined DDoS and malware attack aimed aimed to take down the Internet

Agenda

- 2018 Review
- 2019 Threats
- What you can do now


DEFENSE IN DEPTH

Continuums of Human Behavior



Human behavior is **complex** and **nuanced**, ranging from unintentional to intentional, and with outcomes ranging from negative, to neutral, to positive.

Incidents Are Not Restricted to Technology

Analog (non-technical) errors

- Loss / Theft of Paperwork
- Loss / Theft of Devices
- Accidental credential disclosure (e.g. writing down passwords)
- Accidental disclosure of sensitive information via conversation
- Insecure data disposal
- Allowing tailgating into secure areas
- Sensitive information left on whiteboard
- Data mailed or faxed to incorrect recipient

Technology-enabled errors

- Falling victim to phishing, vishing, and SMiShing attacks
- Data accidently sent to incorrect email recipient
- Failure to use BCC when sending email
- Poor password hygiene
- Malicious app download
- Insecure coding
- Misconfiguration of cloud storage
- Failure to redact data
- Oversharing on social media

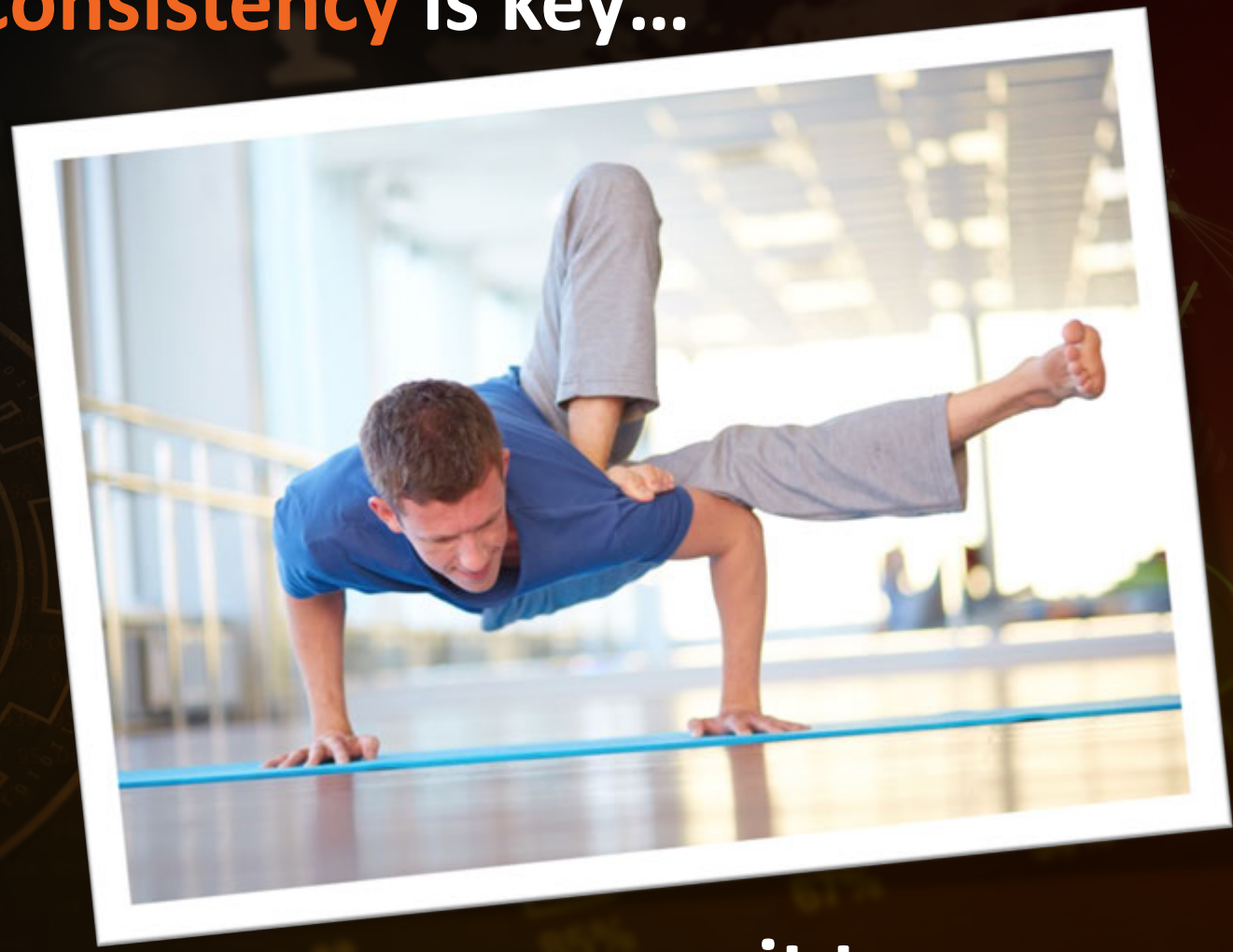
Security Incident or Data Breach

Think about the difference between an **event** and an **ongoing effort**...

... and the difference between a **sprint** and a **marathon**

Be a realistic optimist!

Consistency is key…



…commit to persevere

Encouraging Data Demonstrates the Inherent Effectiveness of Consistency

KnowBe4 Study -- Jan, 2018

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)
- Allowing for a '**follow-the-user-result**' from initial PST baseline, to results after 90 days of combined CBT and phishing training, to the result after one year of combined phishing and CBT

Industries

Energy & Utilities
Financial Services
Business Services
Technology
Manufacturing
Government
Healthcare & Pharmaceuticals
Insurance
Not For Profit
Education
Retail & Wholesale
Other

Size ranges

1 – 249
250 – 999
1000+

For this study, the approximate number of organizations in each size range were as follows:

1 – 249 employees (~8K organizations)
250 – 999 employees (~2K organizations)
1000+ (~1K organizations)

Benchmark Phish Prone Percentage by Industry

Baseline Phish Prone Percentage (B-PPP)			
Industry	**1 – 249 employees**	**250 – 999 employees**	**1000+ employees**
Energy & Utilities	31.56	29.34	22.77
Financial Services	27.41	28.47	23.00
Business Services	29.80	31.01	19.40
Technology	30.68	30.67	28.92
Manufacturing	33.21	31.06	28.71
Government	29.32	25.12	20.84
Healthcare & Pharmaceuticals	29.80	27.85	25.60
Insurance	35.46	33.32	29.19
Not For Profit	32.63	25.94	30.97
Education	29.20	26.23	26.05
Retail & Wholesale	31.58	30.91	21.93
Other	30.41	28.90	22.85

27%

Avg. Initial Baseline PPP

across all industries and sizes

Average PPP by Size of Organization

Org Size	Initial PPP
1 - 249	30.1 %
250 - 999	28.5 %
1000+	25.06 %

*Percentages are calculated for users who experienced a combination of CBT *and* at least 10 phishing tests.*

Results after 1 Quarter of CBT and Phishing Testing

Baseline Phish Prone Percentage (B-PPP)			
Industry	**1 – 249 employees**	**250 – 999 employees**	**1000+ employees**
Energy & Utilities	12.53	13.31	13.40
Financial Services	10.01	9.09	14.53
Business Services	12.89	13.99	13.86
Technology	14.12	16.93	19.83
Manufacturing	13.87	14.24	9.88
Government	13.13	12.76	7.90
Healthcare & Pharmaceuticals	16.81	11.02	15.79
Insurance	13.39	16.49	13.23
Not For Profit	16.01	17.28	17.07
Education	16.95	17.16	22.56
Retail & Wholesale	13.39	10.47	10.49
Other	14.86	16.37	19.97

13.3%

Avg. 90 Day PPP

across all industries and sizes

Average PPP by Size of Organization

Org Size	Initial PPP
1 - 249	13.11 %
250 - 999	13.20 %
1000+	14.10 %

*Percentages are calculated for users who experienced a combination of CBT *and* at least 10 phishing tests.*

Results after 12 Months of CBT and Phishing Testing

Baseline Phish Prone Percentage (B-PPP)			
Industry	**1 – 249 employees**	**250 – 999 employees**	**1000+ employees**
Energy & Utilities	2.83	1.87	5.56
Financial Services	1.54	2.22	5.81
Business Services	1.89	3.09	1.27
Technology	2.02	2.42	2.69
Manufacturing	2.16	3.13	2.47
Government	1.87	1.46	1.52
Healthcare & Pharmaceuticals	2.00	1.65	2.17
Insurance	2.23	2.68	5.26
Not For Profit	2.47	2.24	3.01
Education	2.80	1.91	5.31
Retail & Wholesale	2.14	1.87	2.68
Other	1.82	3.18	4.21

2.17%

Avg. One Year PPP

across all industries and sizes

Average PPP by Size of Organization

Org Size	Initial PPP
1 - 249	1.94 %
250 - 999	2.21 %
1000+	3.04 %

*Percentages are calculated for users who experienced a combination of CBT *and* at least 10 phishing tests.*

Resources

Free IT Security Tools

- Domain Doppelgänger
- Awareness Program Builder
- Domain Spoof Tool
- Mailserver Security Assessment
- Phish Alert
- Ransomware Simulator
- Weak Password Test
- Phishing Security Test
- Second Chance
- Email Exposure Check Pro
- Training Preview
- Breached Password Test

Whitepapers

Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.

Thank You!

Stu Sjouwerman – Founder & Chief Executive Officer, KnowBe4
stus@knowbe4.com

Perry Carpenter – Chief Evangelist & Strategy Officer, KnowBe4
perryc@knowbe4.com