TENTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

THE RIPPLE EFFECT

The Cascading Impacts of Cyber Security

OCTOBER 26–28, 2020

cybersecuritysummit.org

10 YEAR ANNIVERSARY

The Six Most Impactful Cyber and Business Tech Trends of 2020 and What it Means for 2021

10/27/2020: 8:20 AM - 8:30 AM

Session # 7040

Jeremy Swenson, MBA, MSST

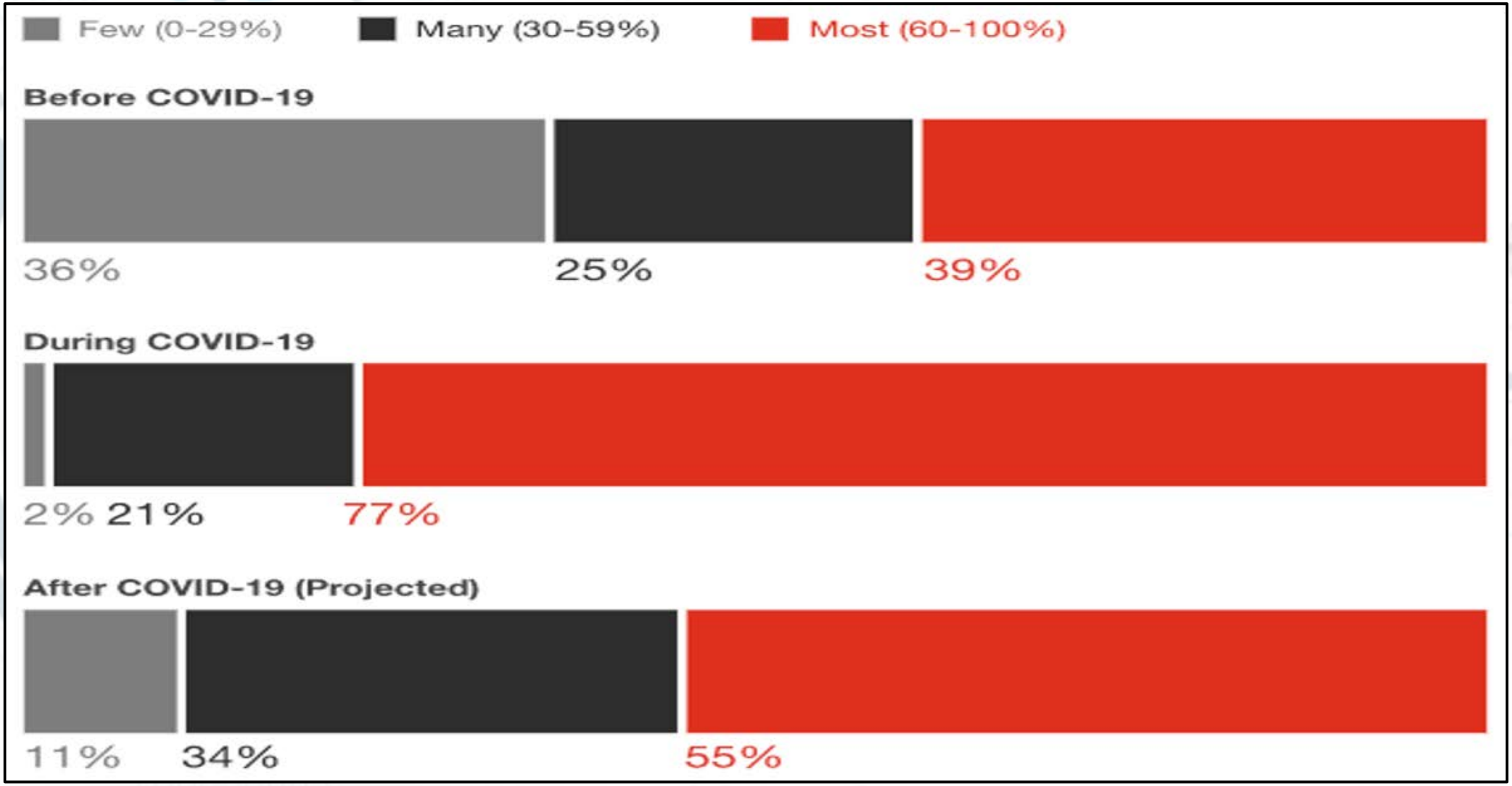
Mamady Konneh, MSST

Agenda

1. Identity & Access Management (IAM)
2. Perimeter Security
3. Data Governance
4. Cloud Security
5. Phishing Attacks
6. Security Automation
7. Takeaways
8. References

Identity & Access Management (IAM)

Fig. 1. What % of Office Employees Do You Think Will WFH at Least 1 Day a Week (PwC, June 2020).

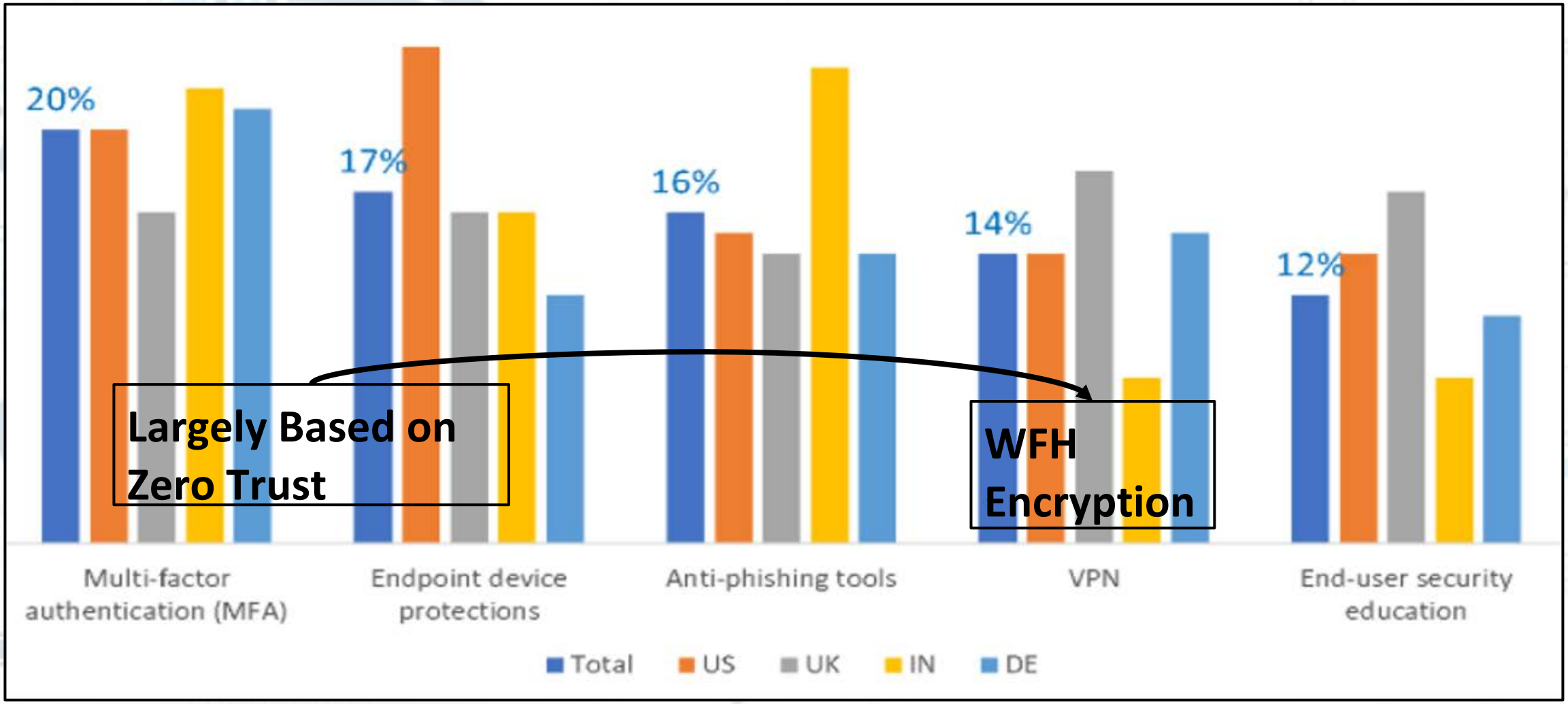


Identity & Access Management (IAM)

1. Mass WFH improves productivity making it likely to become the new norm.
2. Yet with new rules and controls.
3. Given this **51%** of business leaders are **speeding up the deployment of Zero Trust capabilities** (Conway, Andrew. Microsoft Security. Aug 2020).

Identity & Access Management (IAM)

Fig 2. Top 5 Cyber Investments Since The Pandemic (Conway, Andrew. Microsoft Security. Aug 2020).



Perimeter Security

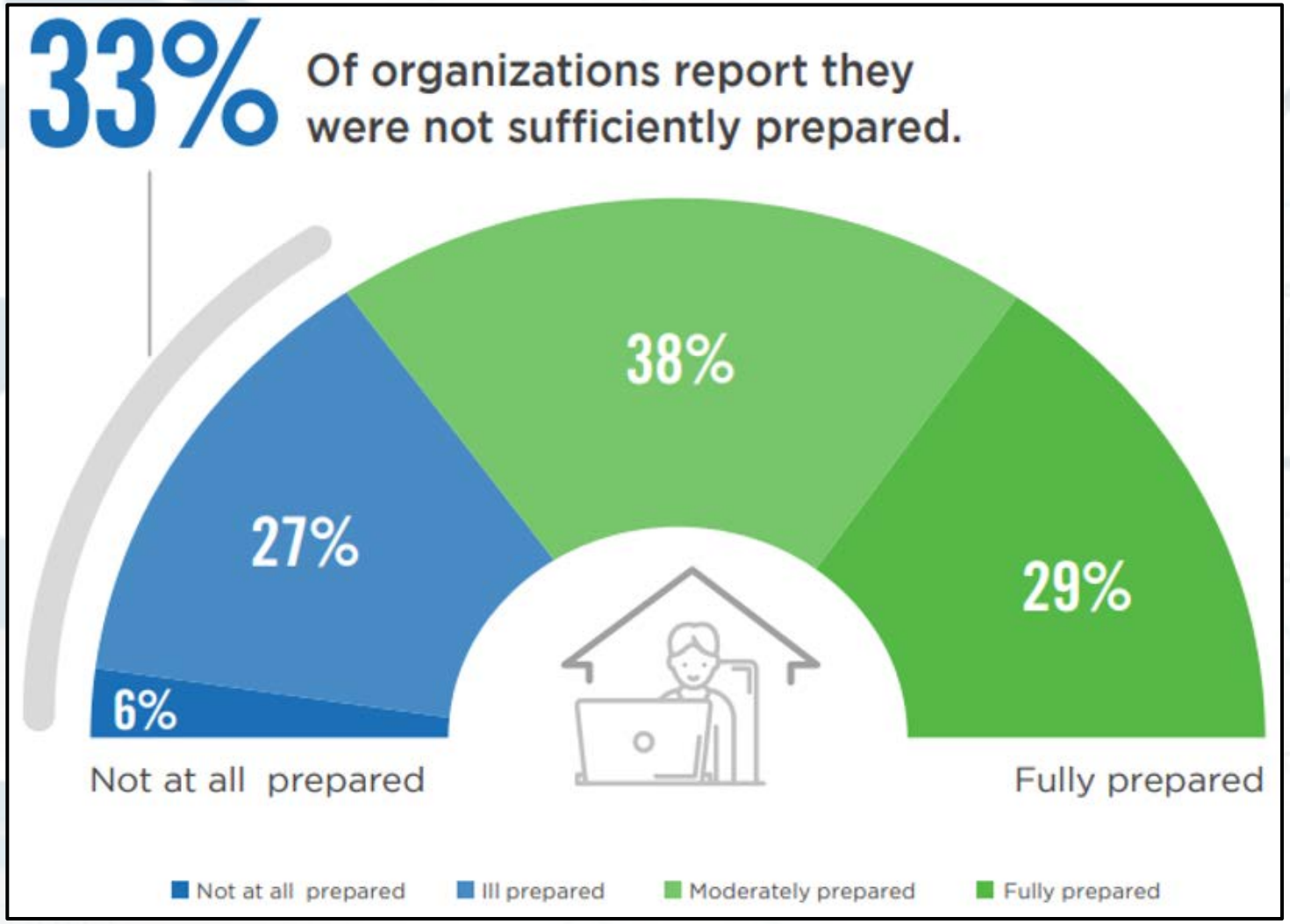
1. Increased WFH Blurs The Perimeter (Physical & Digital)
   a. New IP addresses, internet volume, routing, and VMs (ripple effect).
   b. Prior audit, security controls, and policy **may be ineffective**.
2. Empty Corporate Offices Increased.
   a. Disable non-critical badge access.
   b. Have extra security in or near server rooms.
3. Vendor Interactions Become More Digital Increasing Risk.
   a. Single connection point for all vendors.
      i. Monitored real time.
   b. Exception policy may need to change.

Data Governance

1. Increased agility (Mass WFH) = **sloppy data governance** (ripple effect).
2. One week after the CARES Act was passed Banks were asked to accept Paycheck Protection Program (PPP) loan applications.
3. Many banks were unprepared to deal with the flood of data from digital applications, financial histories, and related docs, thus **not processing them in a efficient way** = **sloppy data governance**.
4. Ease of regulatory enforcement at hospitals/clinics = **sloppy data governance**.
5. Yet don't expect regulators to give you a break.

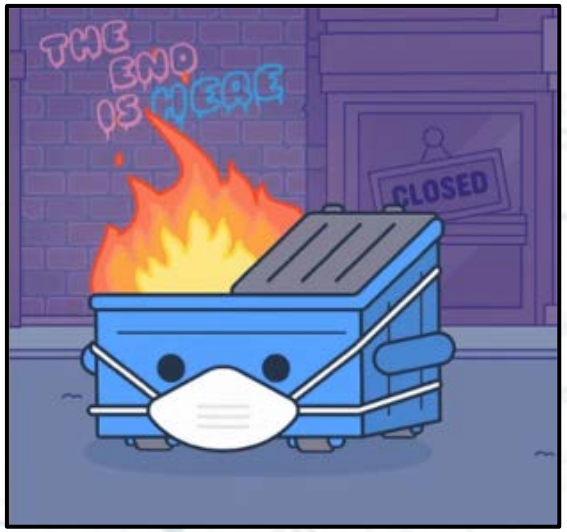
Cloud Security

Fig 3. How Prepared Was Your Org Prior To COVID For Mass Work From Home Scaling (Remote Work From Home Cyber Security Report. (Schultz, Holger. Cyber Security Insiders. Aug 2020).



Cloud Security

1. Hasty rush to bigger cloud scale
   a. Could set stage for 'cyber pandemic' (ripple effect)
      i. Integration issues
      ii. Unclear compliance
      iii. Hidden costs
   b. opportunity to learn and innovate
2. Planned option for bigger cloud scale
   a. Configurations mostly already set
   b. Costs pre negotiated
   c. Better compliance
   d. Less complexity



Sparkles Home of the Dumpster Fire. (Truck Torrence. Giphy. Oct 2020).

Campfire with Marshmallows. (Dreamstime Stock Photos. Oct 2020)

Phishing Attacks

1. Phishing email increases **6,000%** (Sjouwerman, Stu; KnowBe4, July 2020; & Vila, Ashkan; & Carruthers, Stephanie. Security Intelligence, April 2020).
2. Ransomware increases **72%** (Security Magazine, July 2020).
3. Mobile vulnerabilities increase **50%** (Security Magazine, July 2020).

Phishing Attacks

1. Phishing email increases **6,000%** (Sjouwerman, Stu; KnowBe4, July 2020; & Vila, Ashkan; & Carruthers, Stephanie. Security Intelligence, April 2020).
2. Ransomware increases **72%** (Security Magazine, July 2020).
3. Mobile vulnerabilities increase **50%** (Security Magazine, July 2020).

Phishing Attacks

Fig 4. Trend of Successful Phishing Attacks During COVID (Conway, Andrew. Microsoft Security. Aug 2020)

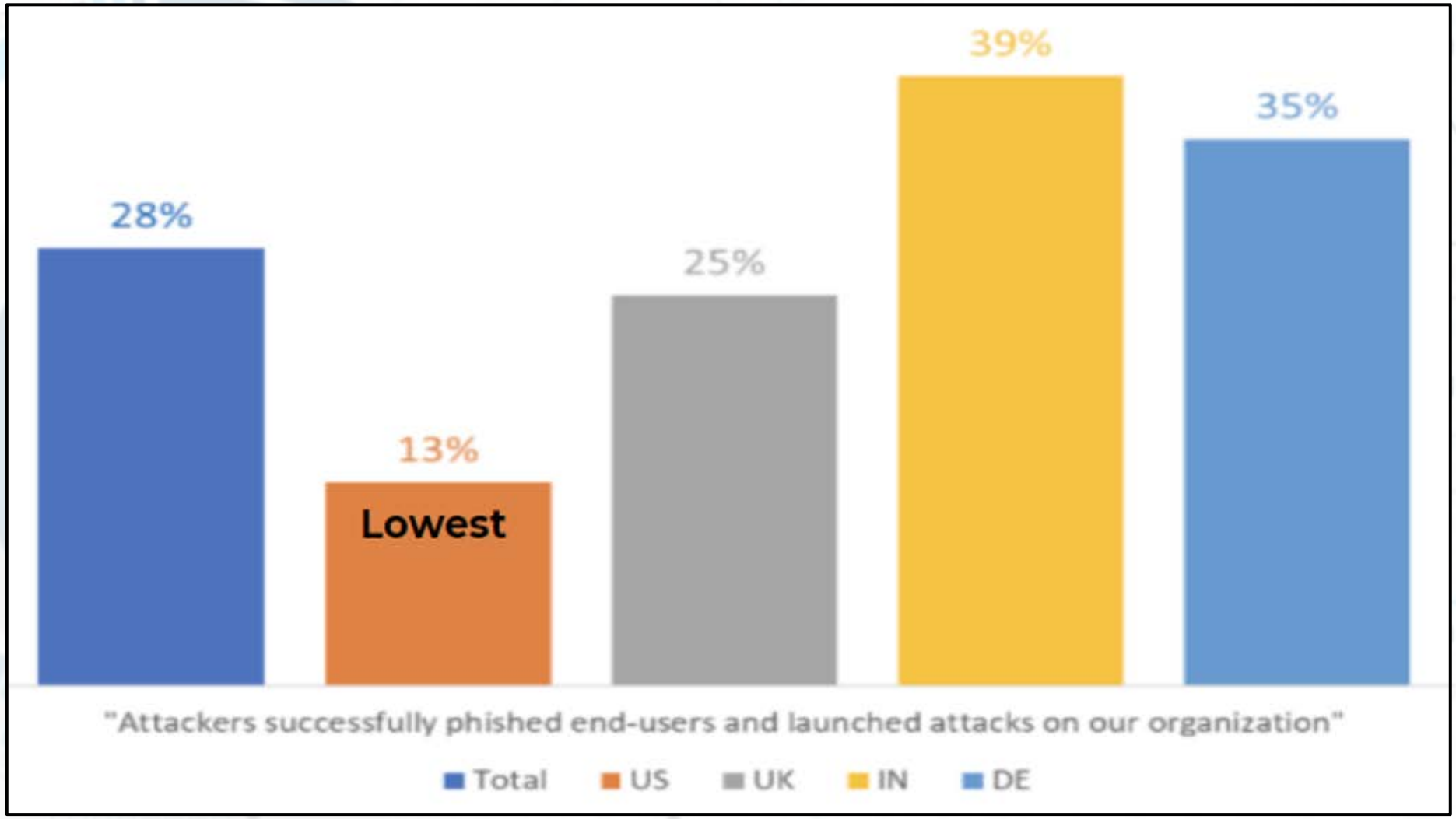
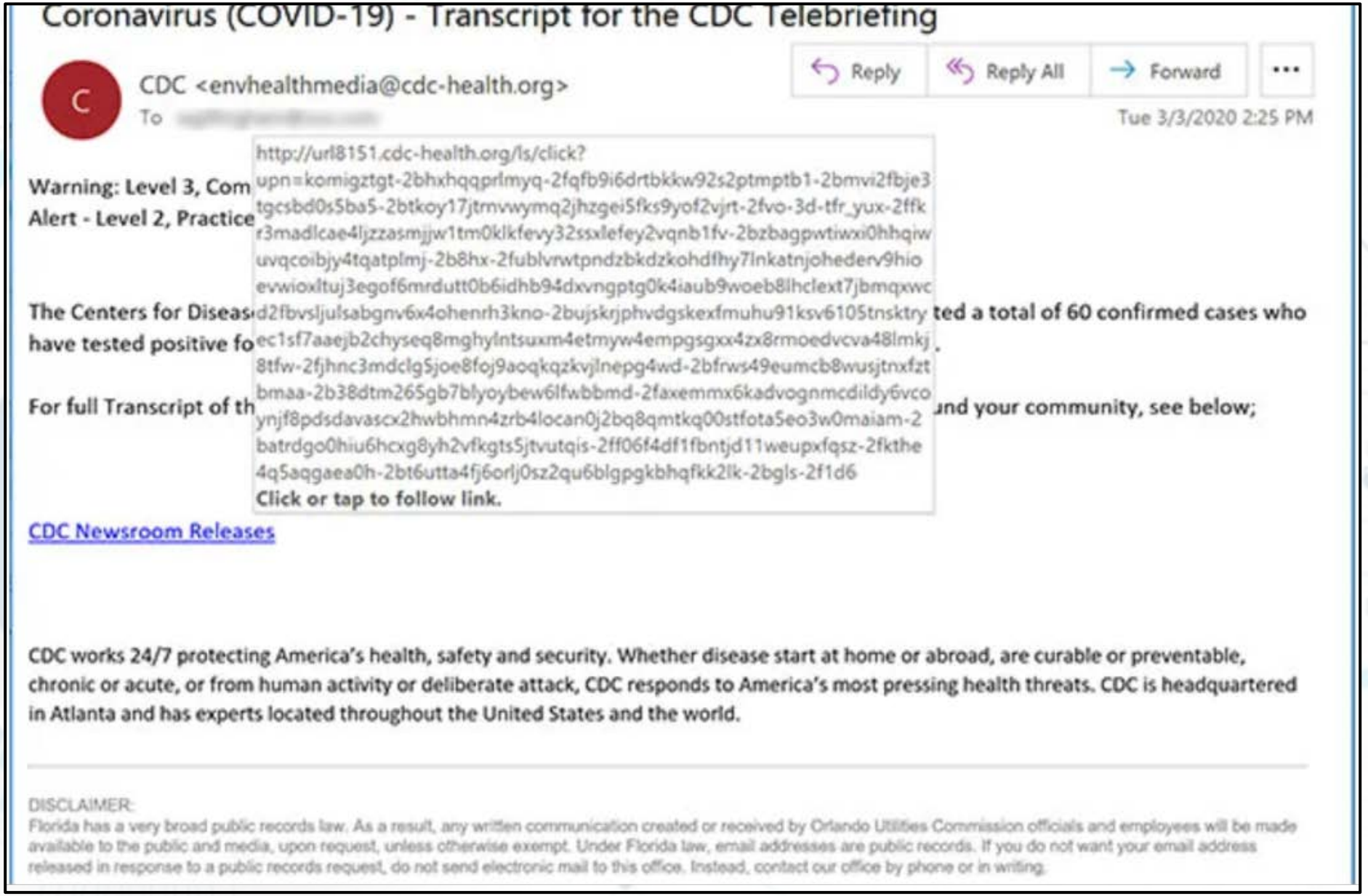


Fig. 5. COVID CDC Phishing Example (KnowBe4, Oct 2020).



Coronavirus (COVID-19) - Transcript for the CDC Telebriefing

CDC <envhealthmedia@cdc-health.org>

To

Reply | Reply All | Forward | ...

Tue 3/3/2020 2:25 PM

Warning: Level 3, Com
Alert - Level 2, Practice

http://url8151.cdc-health.org/ls/click?
upn=komigztgt-2bhxhqqprlmyq-2fqfb9i6drtbkkw92s2ptmptb1-2bmvi2fbje3
tgcsbd0s5ba5-2btkoy17jtrnvwymq2jhzgei5fks9yof2vjrt-2fvo-3d-tfr_yux-2ffk
r3madlcae4ljzzasmjjw1tm0klkfevy32ssxlefey2vqnb1fv-2bzbagpwtiwxi0hhqiw
uvqcoibjy4tqatplmj-2b8hx-2fublvrwtpndzbkdzkohdfhy7lnkatnjohederv9hio
evwioxltuj3egof6mrdutt0b6idhb94dxvngptg0k4iaub9woeb8lhclext7jbmqxwc
d2fbvsljulsabgnv6x4ohenrh3kno-2bujskrjphvdgskexfmuhu91ksv6105tnsktry
ec1sf7aaejb2chyseq8mghylntsuxm4etmyw4empgsgxx4zx8rmoedvcva48lmkj
8tfw-2fjhnc3mdclg5joe8foj9aoqkqzkvjlnepg4wd-2bfrws49eumcb8wusjtnxfzt
bmaa-2b38dtm265gb7blyoybew6lfwbbmd-2faxemmx6kadvognmcdildy6vco
ynjf8pdsdavascx2hwbhmn4zrb4locan0j2bq8qmtkq00stfota5eo3w0maiam-2
batrdgo0hiu6hcxg8yh2vfkgts5jtvutqis-2ff06f4df1fbntjd11weupxfqsz-2fkthe
4q5aqgaea0h-2bt6utta4fj6orlj0sz2qu6blgpgkbhqfkk2lk-2bgls-2f1d6
Click or tap to follow link.

The Centers for Diseas ted a total of 60 confirmed cases who have tested positive fo .

For full Transcript of th and your community, see below;

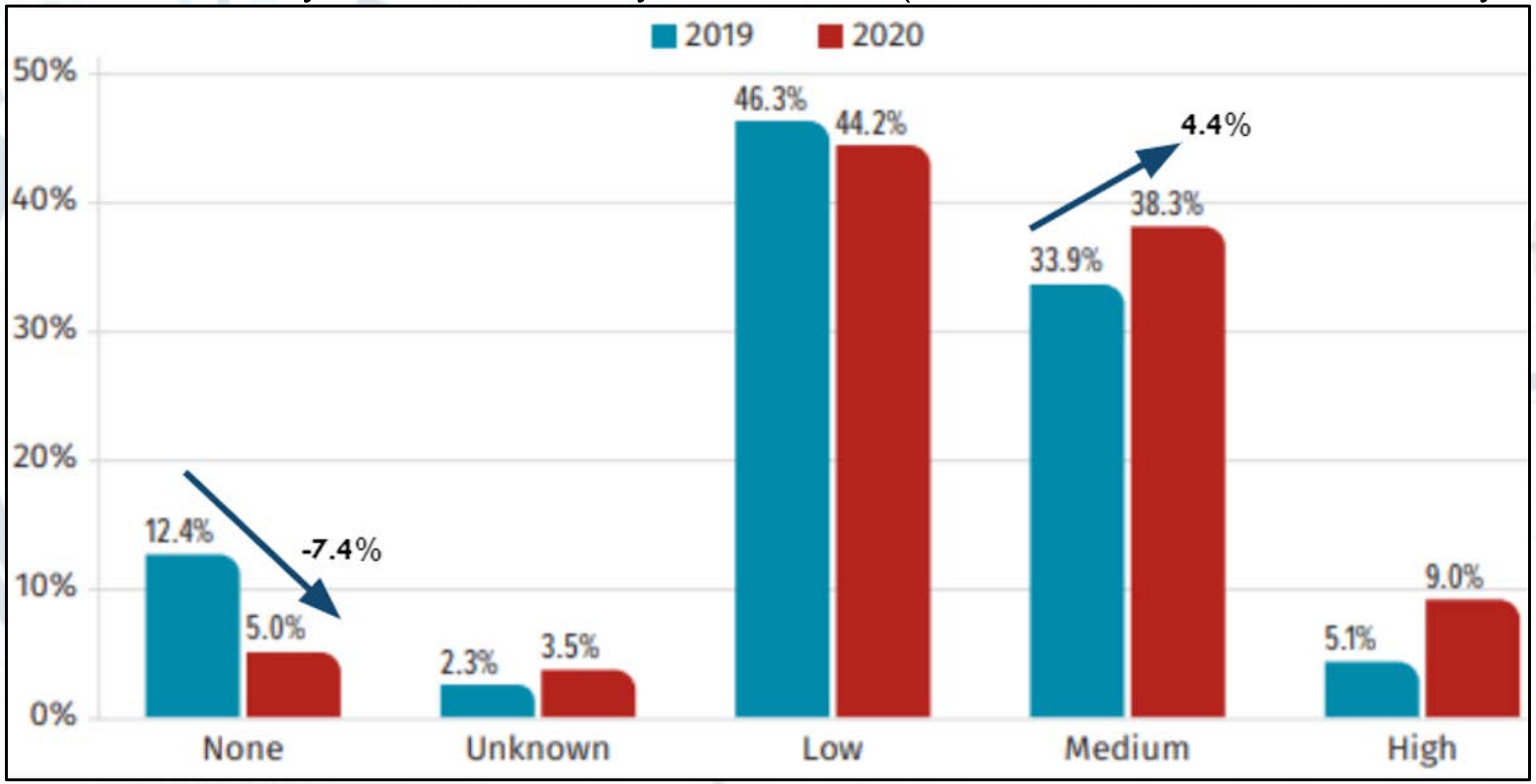
CDC Newsroom Releases

CDC works 24/7 protecting America's health, safety and security. Whether disease start at home or abroad, are curable or preventable, chronic or acute, or from human activity or deliberate attack, CDC responds to America's most pressing health threats. CDC is headquartered in Atlanta and has experts located throughout the United States and the world.

DISCLAIMER:
Florida has a very broad public records law. As a result, any written communication created or received by Orlando Utilities Commission officials and employees will be made available to the public and media, upon request, unless otherwise exempt. Under Florida law, email addresses are public records. If you do not want your email address released in response to a public records request, do not send electronic mail to this office. Instead, contact our office by phone or in writing.

Security Automation

Fig 6. Levels of Security Automation Survey 2019 to 2020 (Don Murdoch, SANs Institute, May 2020).



Security Automation

Fig 7. Automated SecOps Survey 2019 to 2020 (Don Murdoch, SANs Institute, May 2020)

Security Operations Activities or Services Supported	In Use	Level of Automation		
		High	Medium	Low
Intrusion detection	86.8%	27.7%	39.3%	19.8%
Vulnerability management	82.0%	28.7%	36.9%	16.4%
Data protection and monitoring	80.0%	20.9%	35.3%	23.8%
Platform health monitoring and support	79.1%	25.3%	30.6%	23.1%
Command function (IR/Analysis)	73.4%	14.7%	31.0%	27.6%
Cyber threat integration	70.3%	17.2%	25.6%	27.5%
Asset and inventory management	69.9%	18.2%	27.6%	24.1%
Initiate and manage incident response	68.8%	19.6%	25.9%	23.3%
Malware analysis	68.3%	19.3%	24.8%	24.2%
Compliance support	65.5%	15.7%	25.7%	24.1%
Audit/Assessment	64.3%	13.5%	25.1%	25.7%
Threat hunting	57.3%	10.9%	23.7%	22.7%
Forensics/E-discovery collection	56.7%	12.1%	22.7%	21.8%
Security posture assessment with a breach attack simulation tool	44.7%	6.5%	16.8%	21.4%
Other	18.9%	6.3%	10.5%	2.1%

Takeaways

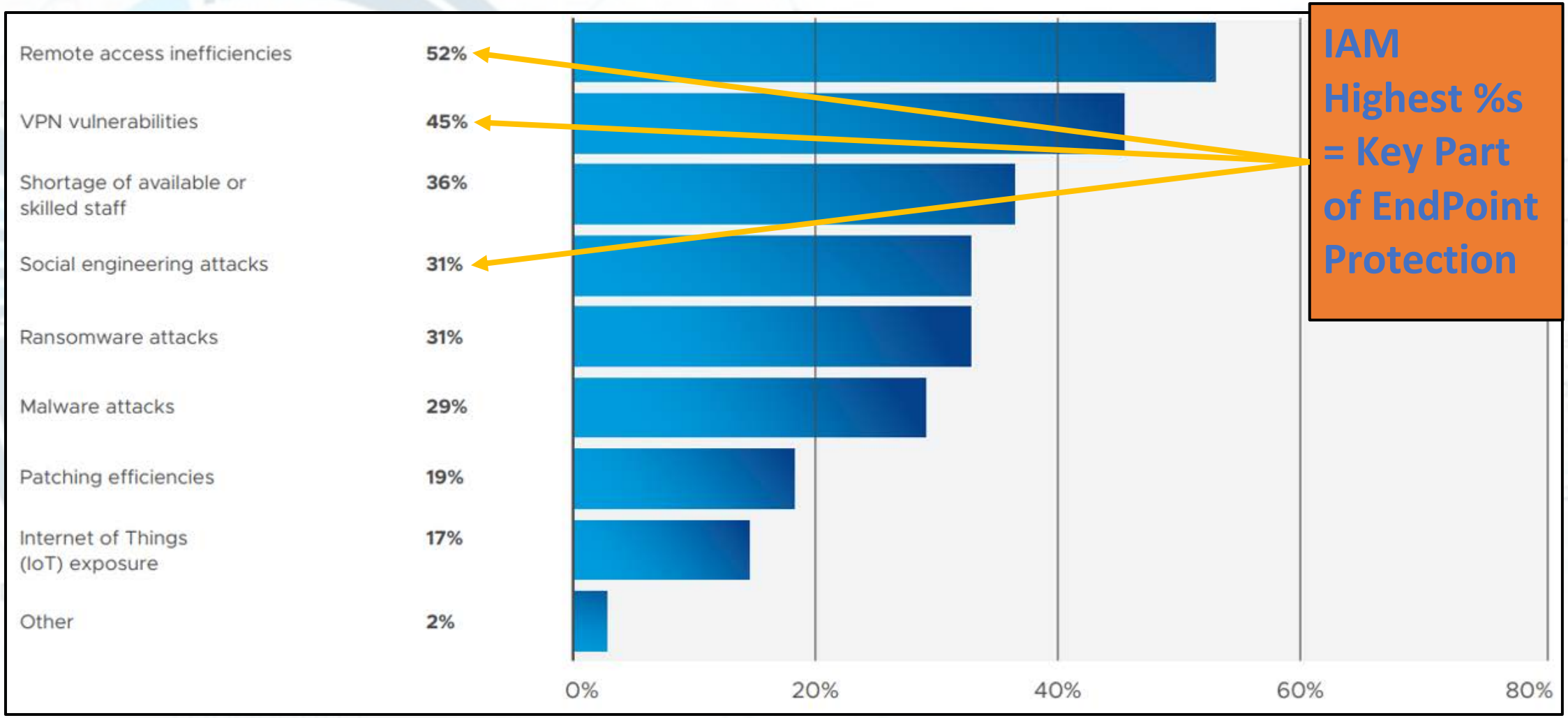
1. COVID-19 is the catalyst for digital transformation in automation, big data, collaboration tools, and AI (ripple effect).
2. We no longer have the same office and thus less badge access needed.
3. Single sign-on (SSO) will expand to personal devices and smartphones/watches.
4. Geolocation based authentication is here to stay with biometrics likely.
5. Security perimeter is now more defined by **data analytics** than **physical/digital boundaries**.
6. Cloud infra will grow fast creating perimeter and compliance complexity / fog.

References

1. PricewaterhouseCoopers (PwC). “PwC’s US Remote Work Survey”. June 2020. https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html
2. Conway, Andrew. “New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security.” Microsoft Security. Aug 2020. https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/
3. Kellermann, Tom; & McElroy, Rick. “Global Incident Response Threat Report: COVID-19 Continues to Create a Larger Surface Area for Cyberattacks - incident response professionals note an increase in counter IR and island hopping”. VMWare & Carbon Black. Aug 2020. https://www.carbonblack.com/wp-content/uploads/VMWCB-Report-COVID-19-Continues-to-Create-a-Larger-Surface-Area-for-Cyberattacks.pdf
4. Schultz, Holger. “Remote Work From Home Cyber Security Report”. Cyber Security Insiders. Aug 2020.
5. Flexera. “2020 Flexera State of the Cloud Report”. Flexera. April 2020. https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020?utm_source=Blog&utm_medium=Blog&utm_campaign=Computing%20Trends&id=Computing-Trends-Blog
6. Sjouwerman, Stu. KnowBe4, July 2020. https://blog.knowbe4.com/6000-increase-in-phishing-attacks-leveraging-covid-19-healthcare-industry-often-the-target
7. Truck Torrence. “Sparkles Home of the Dumpster Fire”. Giphy. Oct 2020. https://giphy.com/gifs/coronavirus-covid-19-dumpster-fire-Ll8wx3yoDKFUblxspY
8. Campfire with Marshmallows. (Dreamstime Stock Photos. Oct 2020).
9. Vila, Ashkan; & Carruthers, Stephanie. Security Intelligence. April 2020.
10. https://securityintelligence.com/posts/new-study-shows-consumers-could-be-vulnerable-to-covid-19-spam/
11. Security Magazine, July 2020: https://www.securitymagazine.com/articles/92886-covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50
12. B4Know. COVID 19 Phishing Examples. Oct 2020. https://www.knowbe4.com/covid-gallery-phishing-examples
13. Murdoch,Don. SANs Institute. “2020 SANS Automation and Integration Survey”. May 2020. https://www.devo.com/sans-automation-integration-survey-2020/

Appendix 1 - Identity & Access Mgmt. (IAM)

The Most Daunting Endpoint Security Challenges Observed Amid COVID-19 (Kellermann, Tom; & McElroy, Rick. VMWare & Carbon Black. Aug 2020).



Appendix 2 - Cloud Security

Pandemic Influenced Cloud Spend Change 2019 to 2020 (Flexera, April 2020).