STROZ FRIEDBERG
an Aon company

AON
Empower Results®

2018 Cybersecurity Predictions

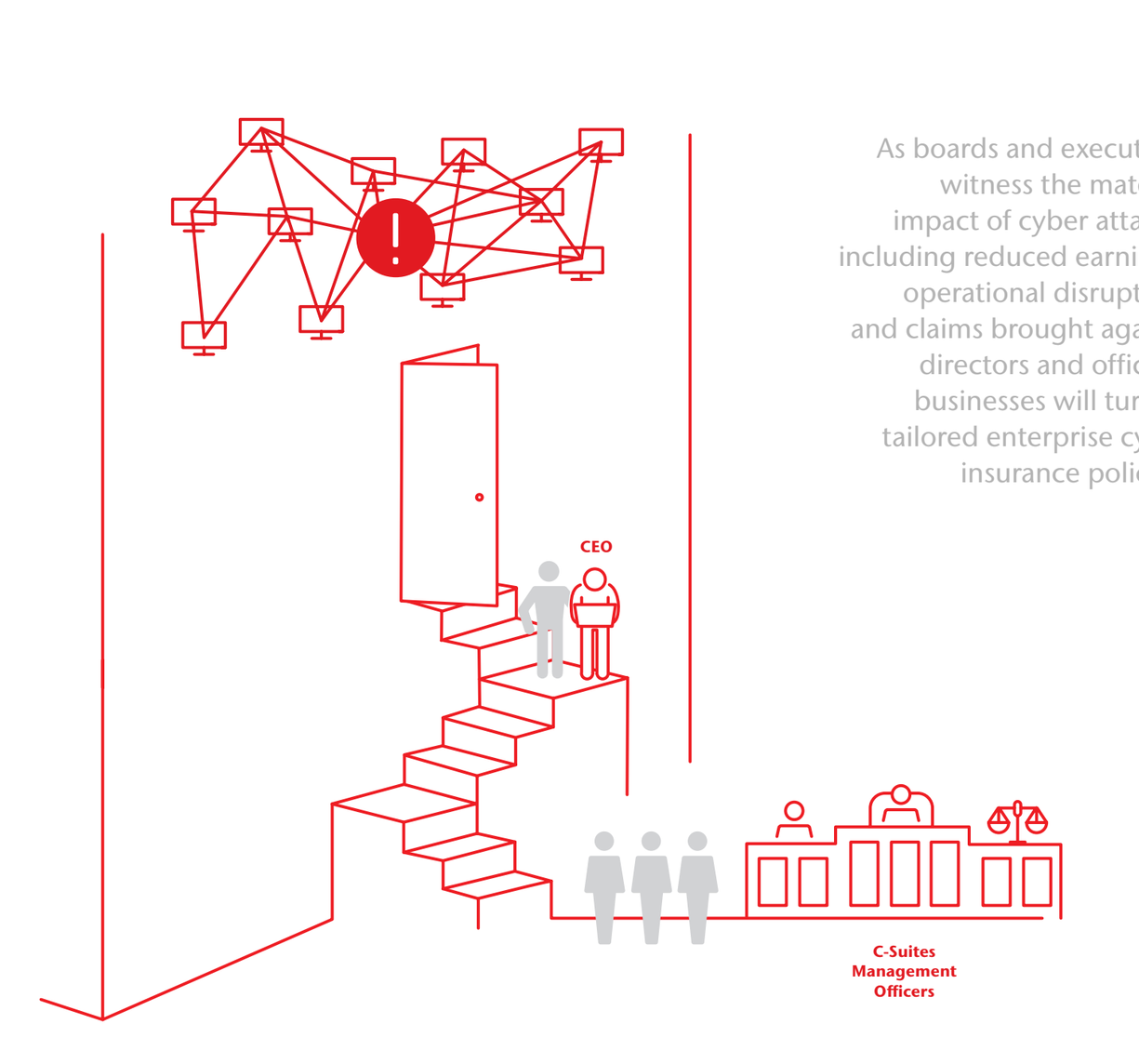
A Shift to Managing Cyber as an Enterprise Risk

#1 Cyber Liability

In 2017, C-suite executives resigned following massive data breaches.

24% of risk management professionals said their companies had cyber insurance

87% of risk management professionals view cyber liability as one of their top ten business risks



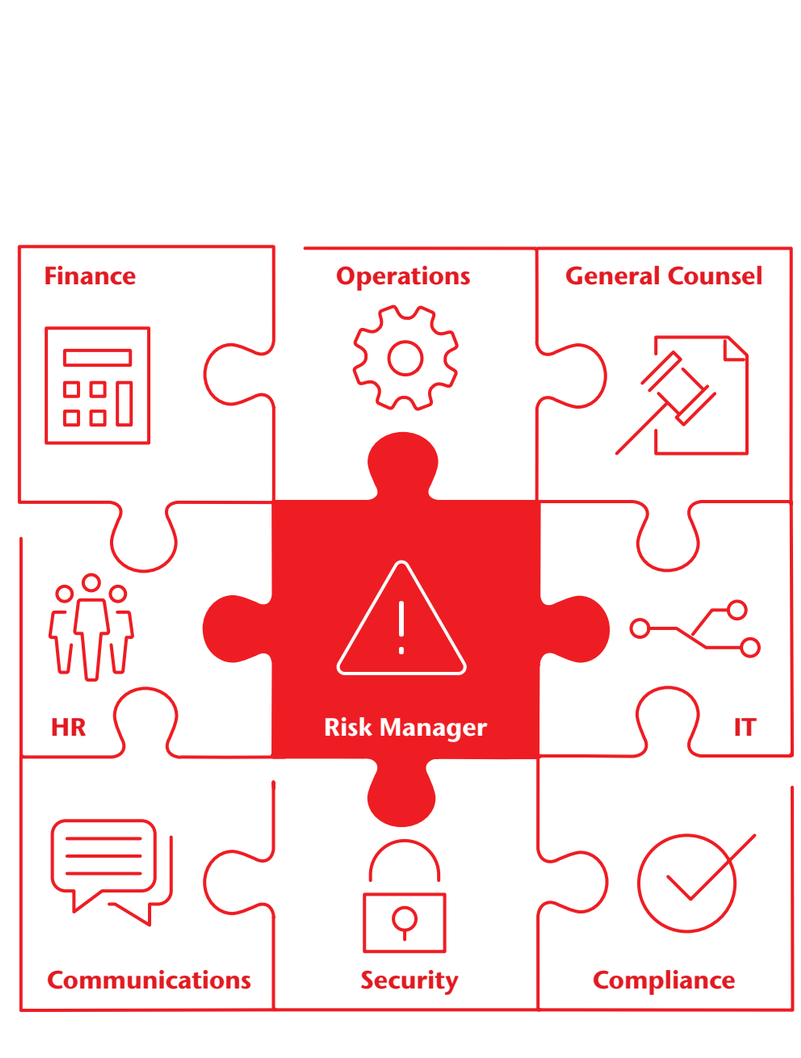
As boards and executives witness the material impact of cyber attacks, including reduced earnings, operational disruption, and claims brought against directors and officers, businesses will turn to tailored enterprise cyber insurance policies.

Businesses adopt standalone cyber insurance policies as boards and executives wake up to cyber liability.

#2 Chief Risk Officers

In 2017, silos abounded in cybersecurity risk management, and criminals exploited the gaps.

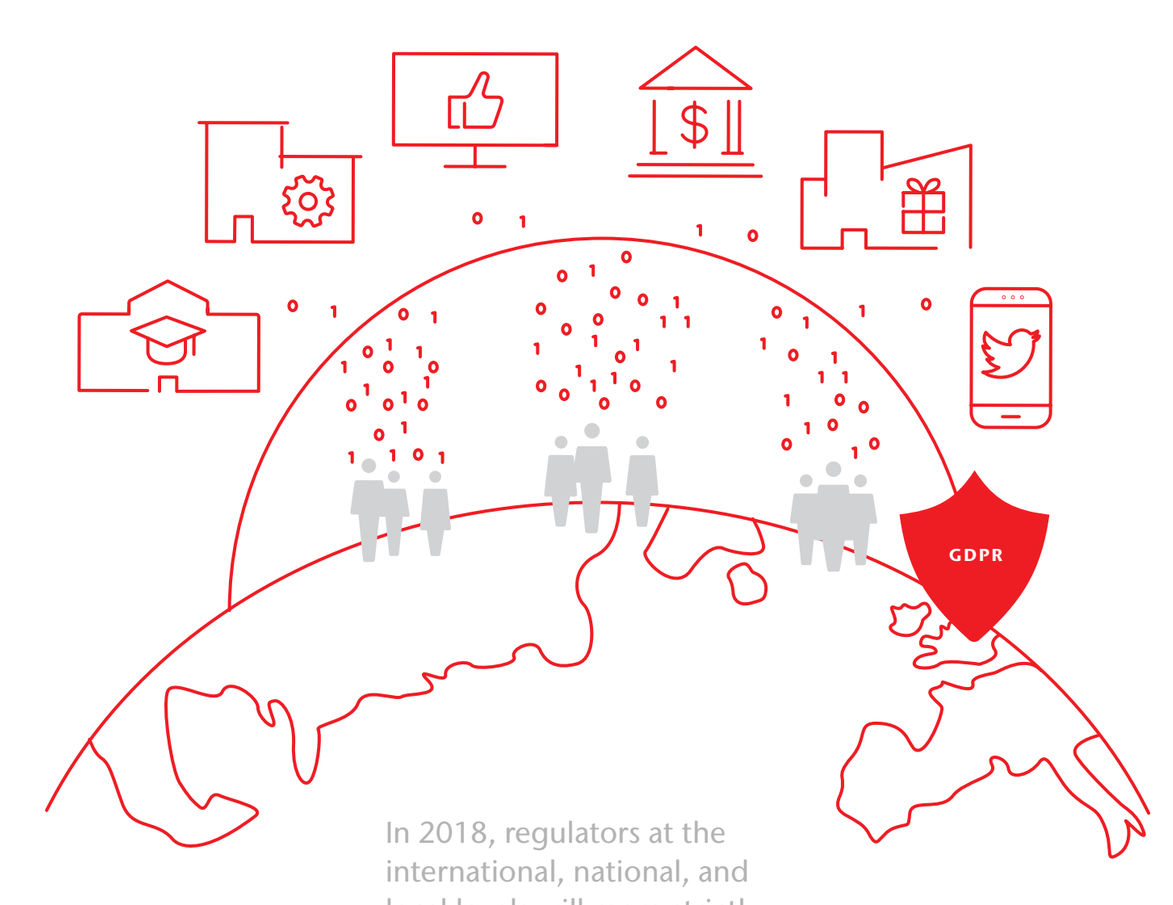
Chief risk officers will work with information security teams, treasurers, chief financial officers, and general counsels to improve risk modeling and paint a more holistic picture of the business' exposure.



As the physical and cyber worlds collide, chief risk officers take center stage to manage cyber as an enterprise risk.

$86.4B was spent on security in 2017, up 7% from the previous year

#3 Regulatory Pressure

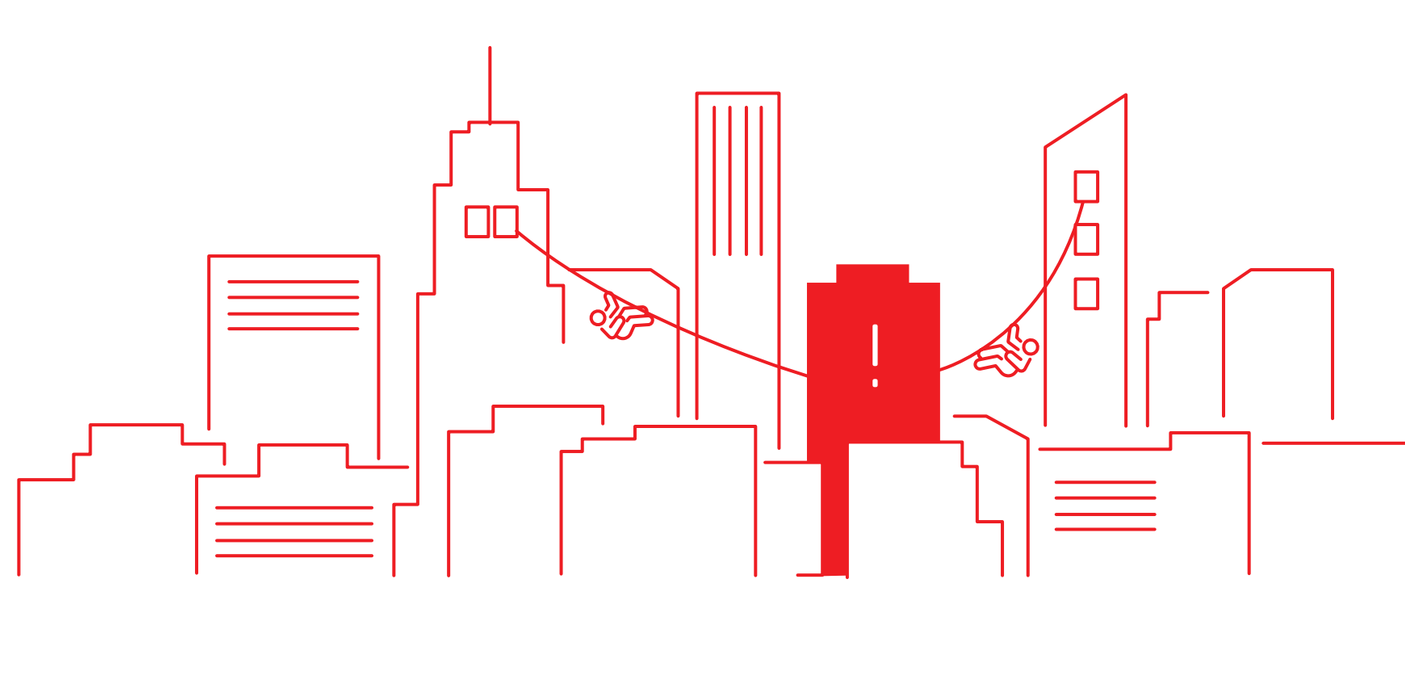


In 2018, regulators at the international, national, and local levels will more strictly enforce existing cybersecurity regulations and increase compliance pressures by introducing new ones.

Regulatory spotlight widens and becomes more complex, provoking calls for harmonization. European Union holds global company to account over GDPR violation; big data aggregators come under scrutiny in the United States.

#4 SMB Cybersecurity

In 2018, we will see an attack on a SMB that has not properly integrated security into its IoT ecosystem, and this attack will extend into the network of a large organization causing exponentially more damage.



Criminals look to attack businesses embracing the Internet of Things, in particular targeting a small to mid-sized company providing services to a global organization.

Even if a company's own IoT ecosystem is relatively secure, the impact of how third parties are deploying IoT is neglected.

55% of small businesses reported to have been breached in a 12-month period between 2015 and 2016

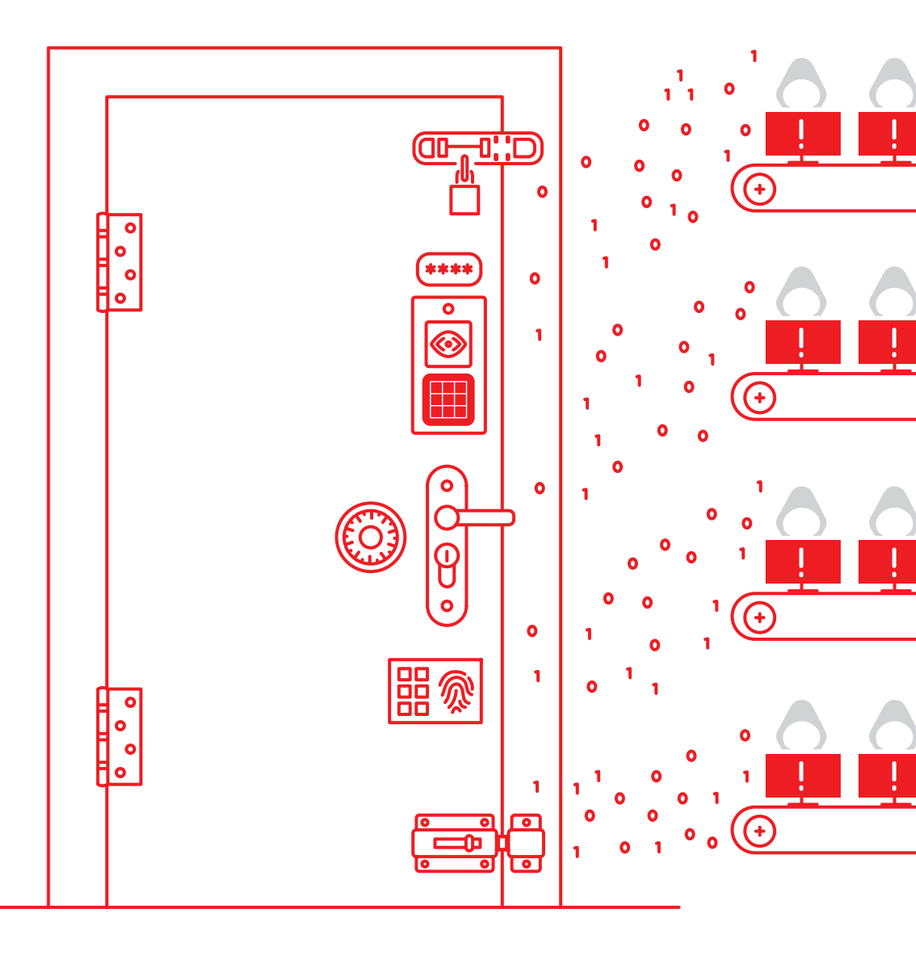
...yet a tiny minority said they view it as the most critical issue they face.

#5 Multi-Factor Authentication

While passwords alone do not provide adequate levels of security, their convenience means that they are still widely deployed.

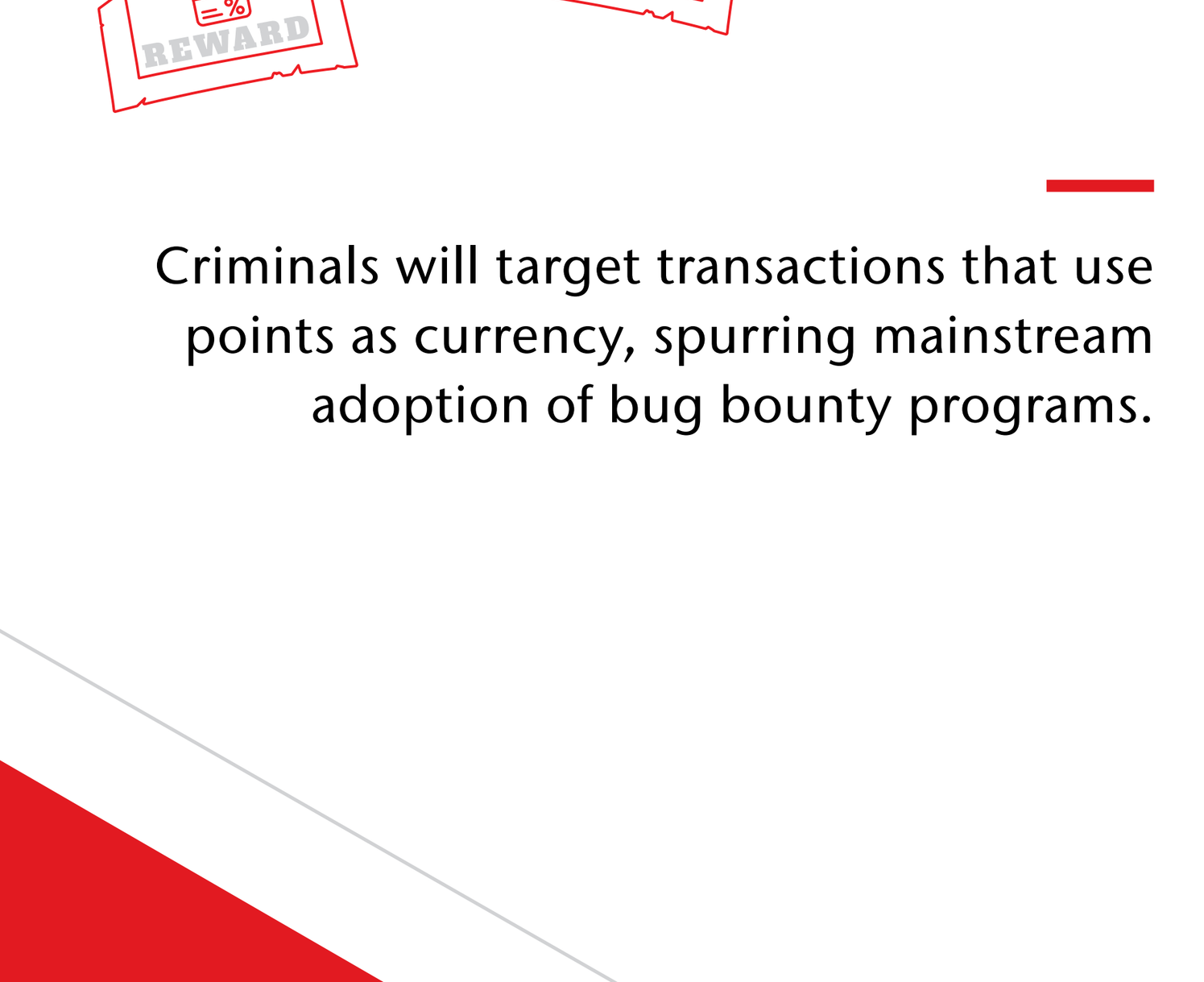
81% of hacking-related breaches leverage stolen or weak passwords

Companies will widely adopt MFA as criminals successfully target single factor authentication, such as usernames and passwords, and biometrics.



As passwords continue to be hacked, and attackers circumvent physical biometrics, multi-factor authentication becomes more important than ever before.

#6 Bug Bounty Programs



Businesses with loyalty, gift, and rewards programs, such as airlines, retailers, and hospitality providers, will be the next wave of adopters as criminals target transactions that use points as currency.

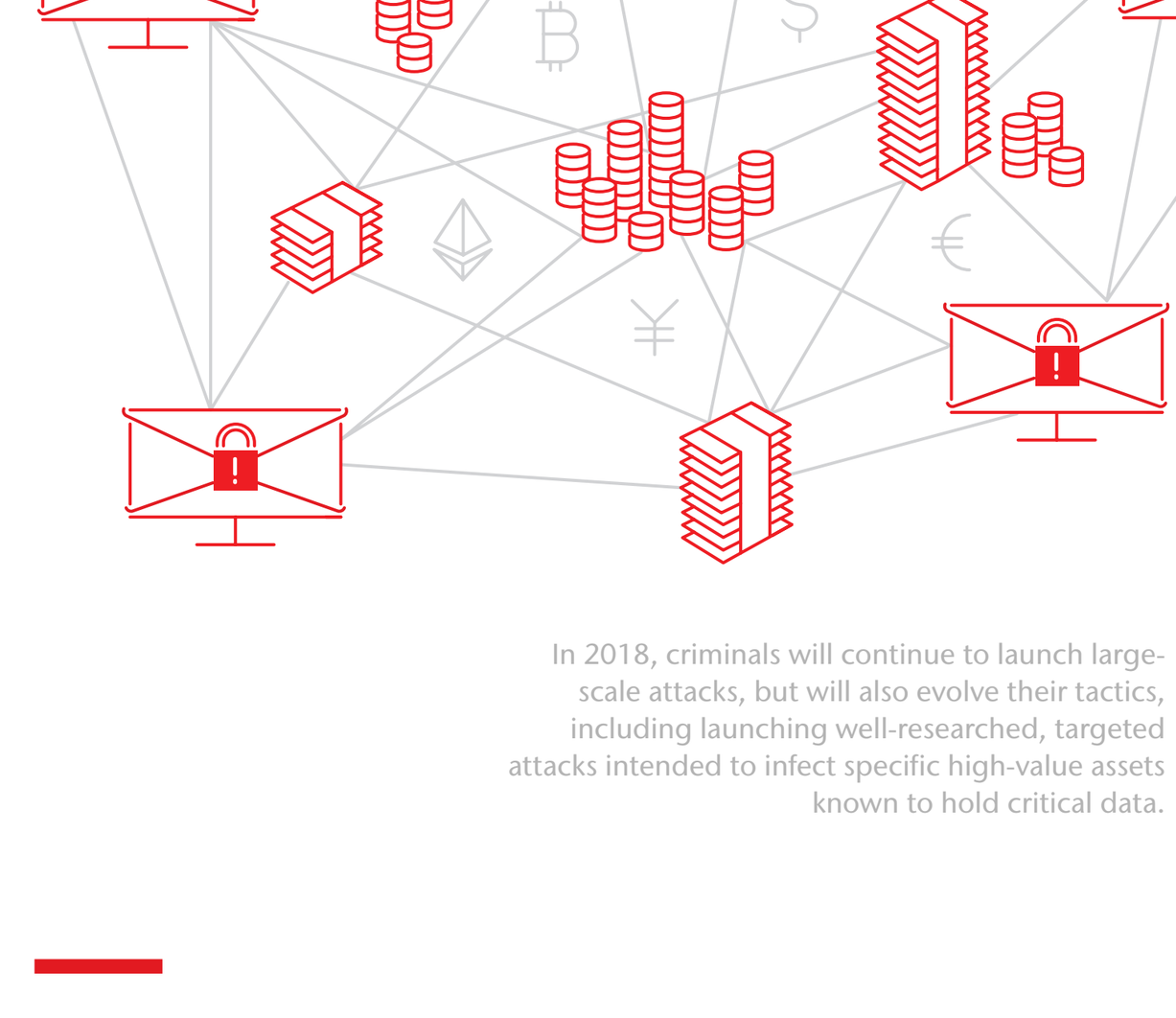
Criminals will target transactions that use points as currency, spurring mainstream adoption of bug bounty programs.

As the threat environment drives broader adoption, bug bounty programs will become part of the standard security lifecycle.

Researchers earned **$70K** for exploiting the bugs in Apple's iOS 11.1

#7 Ransomware Attacks

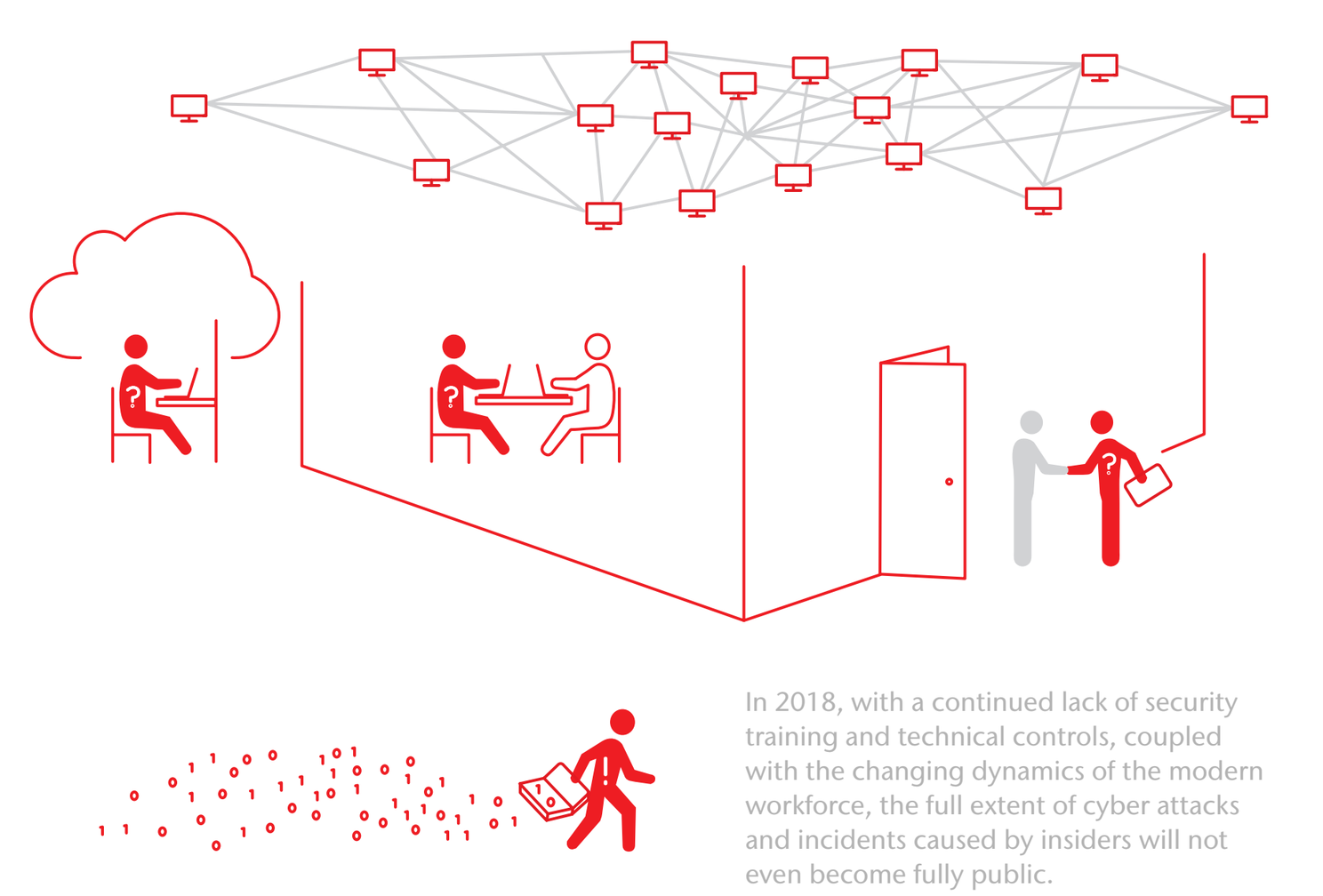
$5B is the estimated global cost for organizations of ransomware attacks in 2017 – up 400% from 2016



In 2018, criminals will continue to launch large-scale attacks, but will also evolve their tactics, including launching well-researched, targeted attacks intended to infect specific high-value assets known to hold critical data.

Ransomware attackers get targeted; cryptocurrencies help ransomware industry flourish.

#8 Insider Risks



In 2018, with a continued lack of security training and technical controls, coupled with the changing dynamics of the modern workforce, the full extent of cyber attacks and incidents caused by insiders will not even become fully public.

Insider risks plague organizations as they underestimate their critical vulnerability and liability, and major attacks continue to fly under the radar.

+ DOWNLOAD THE REPORT

www.aon.com | www.strozfriedberg.com