KIVU

American Home Furnishings Alliance
Cyber Threat Insights
November 12, 2021

Agenda

- Introductions
- Top Cyber Trends
- Ransomware Briefing
- Wire Transfer Fraud Briefing
- Cyber Strategy

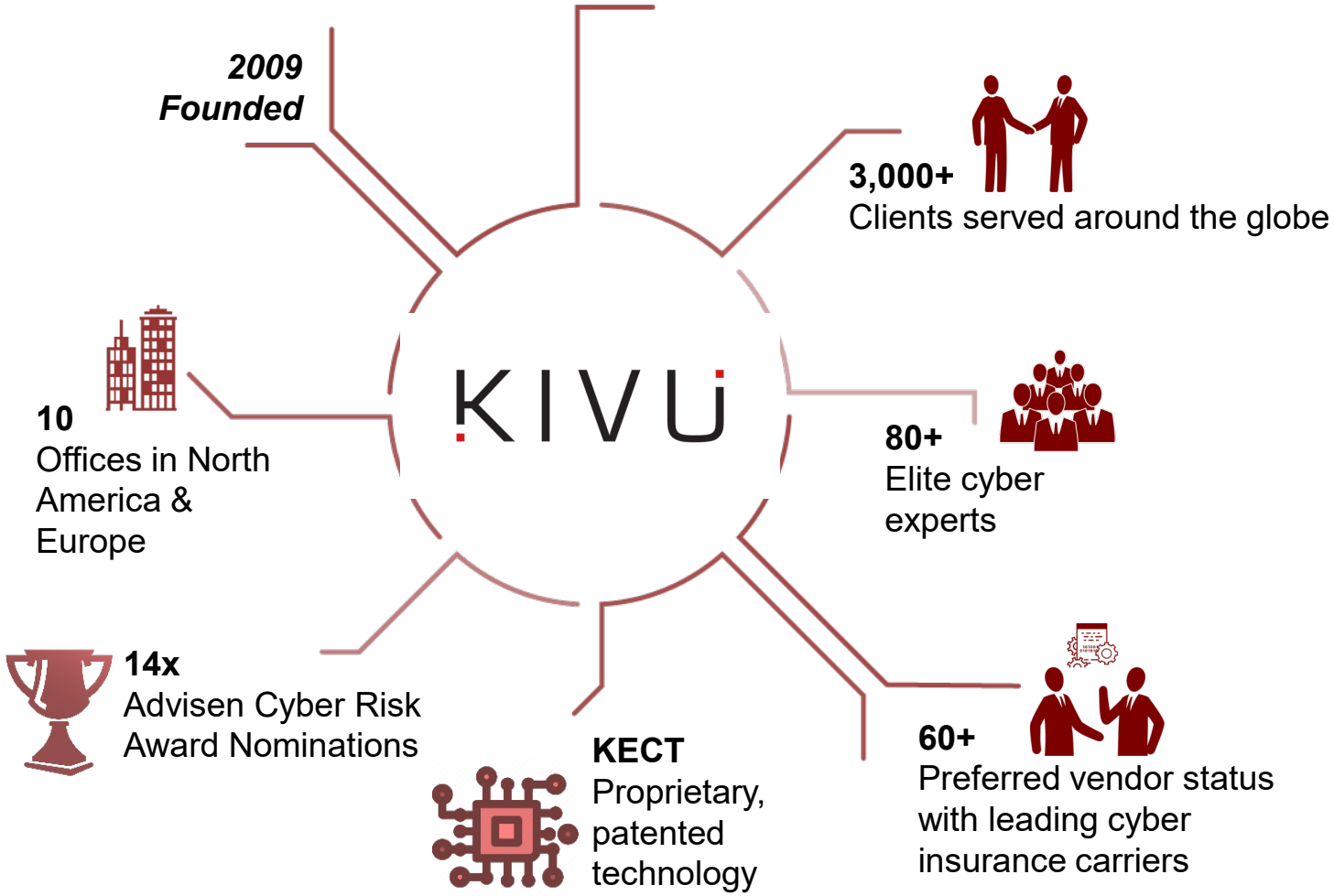
Dustin Owens

Dustin Owens is the VP of Cyber Risk & Resilience capabilities, which focus on proactive/pre-breach services at Kivu. Dustin has over 25 years of cyber experience with his core expertise being enterprise risk management and compliance. Dustin's industry expertise comes in the form of financial services, energy, healthcare, manufacturing, retail, travel and transportation, hospitality and consumer packaged goods.

Prior to joining Kivu, Dustin held various service leadership positions at Lucent Technologies, International Network Services, British Telecom, HP/DXC and Optiv Security.

Kivu Background

KIVU



Cyber Security

Evolution & Current State of
Cyber in Manufacturing

Top Cyber Threats

Manufacturing

- Top Threat Events
  - Ransomware
  - Wire transfer fraud
- Top Manufacturing Attack Tactics (How)
  - System Intrusion
  - Social Engineering (phishing)
  - Basic Web Application Attacks
- Top Threat Actors (Where):
  - External (82%), Internal (19%), Multiple (1%)

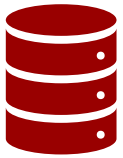
*Source: *2021 Verizon Data Breach Investigation Report*

KIVU

Ransomware

Industry Threat Briefing

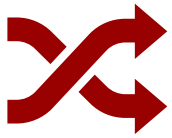
Ransomware Primer



Critical / Sensitive Data Encrypted

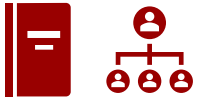
Pay / No Pay Decisions

Issuance of Ransom Note



Double Extortion Schemes

Imposed Time Limitations



Research by Attackers

Ransom Impacts

- Average Duration of Negotiations – 9 Days
- Average Initial Ransom Demand in US Dollars* – $892k
- Average Initial Ransom Demand for Companies > $500M in Revenue - $3M
- Average Cost of a Ransomware Breach - $4.62M (not including ransom payment)**
- 51% of Manufacturing Sector Experienced Significant Revenue Loss Post Breach***

Engaging with Ransomware Agents

- Exercising caution with self engagement
- Profiling a threat actor
- Office of Foreign Assets Control (OFAC) Check
- Negotiation Objectives
  - Delaying payment timeline
  - Ransom reduction
  - Digital payment process

KIVU

Wire Transfer Fraud

Industry Threat Briefing

Payment Fraud Statistics

74%

Organizations Experiencing Payments Fraud in 2020

$50,000 or less

Total for Most Organizations Suffering a Business Email Compromise (BEC) attack

30%

Organizations Experiencing Increase of Incidents in 2020

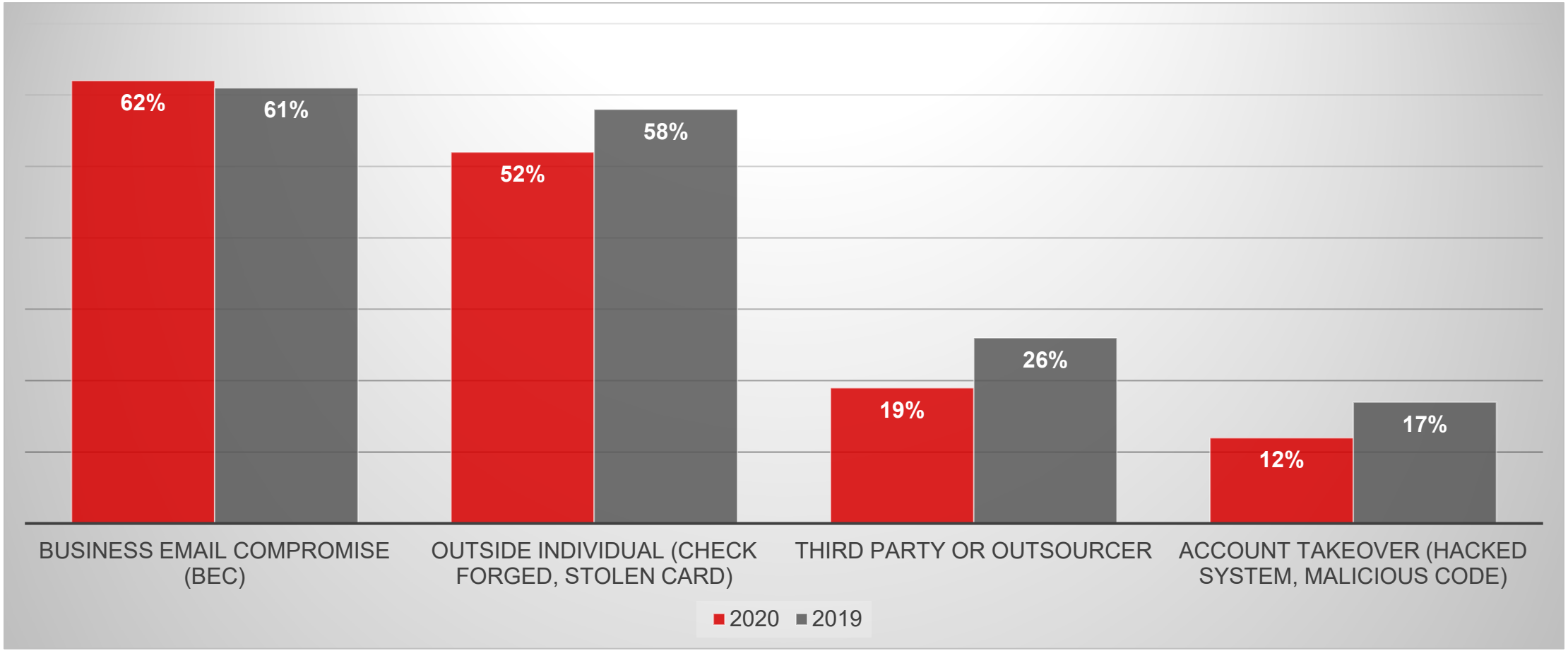
Accounts Payable

Department Most Targeted for Business Email Compromise Attacks

*Source: *2021 Association for Financial Professionals Payments Fraud and Control Survey Report*

Sources of Payments Fraud

% Experiencing Sources of Actual or Attempted Fraud



*Source: *2021 Association for Financial Professionals Payments Fraud and Control Survey Report*

Business Email Compromise (BEC)

Common Types of BEC Attacks

- Emails from third parties requesting bank changes, payments instruction, etc
- Emails from fraudsters posing as senior executives requesting transfer of funds
- Emails from fraudsters impersonating as vendors

*Source: *2021 Association for Financial Professionals Payments Fraud and Control Survey Report*

KIVU

Cyber Strategy

Industry Threat Briefing

Strategic Cyber Recommendations

- Focus first on fixing common attack points
- Incorporate a risk-based approach to cyber
- Conduct regular cyber threat briefings for the board
- Stay apprised of trends with cyber insurance underwriting requirements
- Specific to ransomware, leverage executive tabletops to fully understand preparedness for pay / no pay decision making

Top Cyber Prevention Tactics

KIVU

Prepare

- Security Awareness and Skills Training
- Business Impact Analyses
- Risk Assessments

Protect

- Multi Factor Authentication
- Patch Management
- End Point Detection & Response

Test

- Phishing Simulations
- Tabletop Exercises
- Penetration Testing

Cyber Risk & Resilience

Proactive Cyber Protection

KIVU