Cybersecurity and Business

Kate Shanks, *Senior Vice President of Public Affairs*, Kentucky Chamber

Bryan M. Cobb, *vCIO / Project Lead*, Cforward

August 17, 2022

Kentucky Chamber

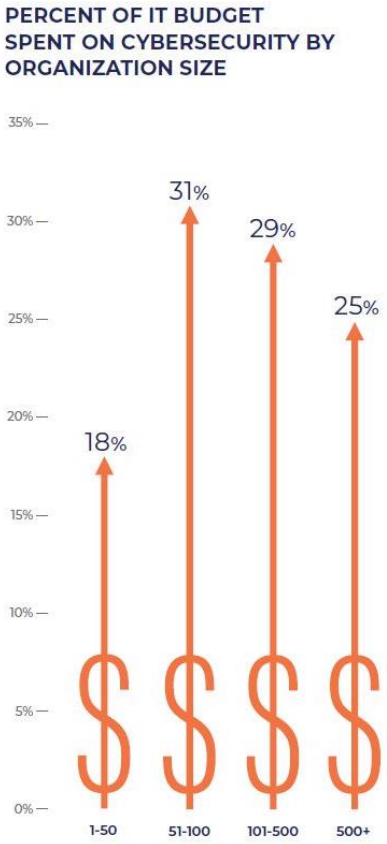
CFORWARD
INFORMATION TECHNOLOGIES

A Look at the Numbers

- Most breaches come from external attacks (80%).
- Attacks motivated by money
- Hardest hit industries: education, government, healthcare, construction, manufacturing
- Small businesses are not immune.

A Look at the Numbers

- 75% of critical infrastructure small and midsized businesses experienced at least one breach in company history.
- Average cost and time to resolve: $170,000 and 7.5 months
- Increase in attacks is leading businesses to take action such as outsourcing cybersecurity.
- Increase staff training, new policies and procedures
- Industry experts recommended to dedicate 10-15% of their IT budget toward cybersecurity depending on needs and risk tolerance; on average most businesses are spending as much if not more.



Kentucky Chamber

FORWARD
INFORMATION TECHNOLOGIES

Common Actions

- Multi-factor authentication (MFA), training for staff, policies and procedures, risk assessments, insurance, and software updates
- Utilizing guidance by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency
- Increased spending

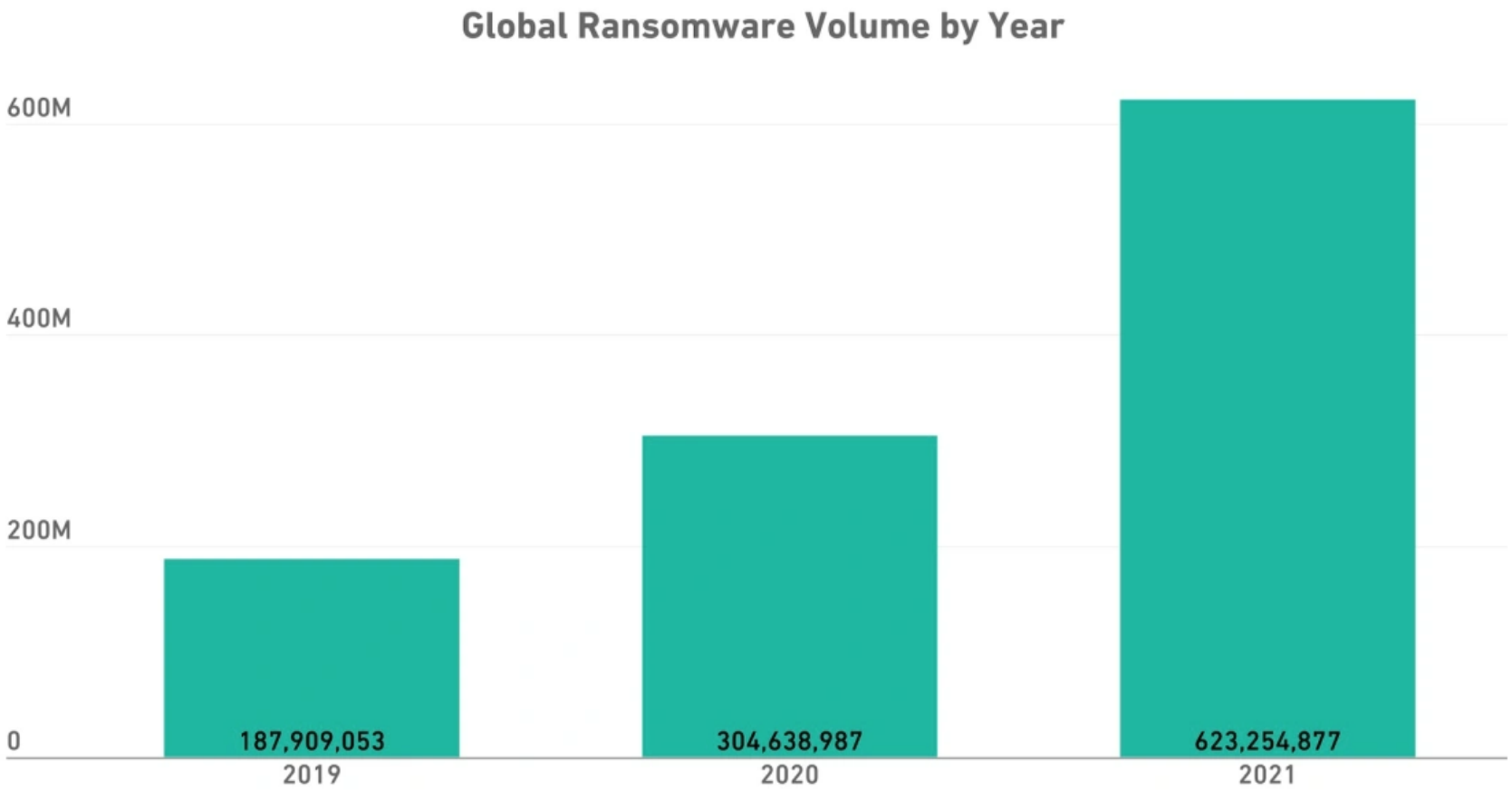
COVID and Changing Workplace

- Working at home
- New government programs (PPP, UI Fraud)
- People are the weakest link; COVID made us weaker

Ransomware Attacks on the Rise

- 2018-2019 attacks grew 500%
- It’s not just fear of a breach but the importance of the data.
- Ransomware is impacting the cybersecurity insurance market.
  - Dynamic and developing quickly; still relatively young market compared to other property and casualty coverages; moving toward stability
  - First policy written in the 90s, mid-2000s policies written to protect the entity itself

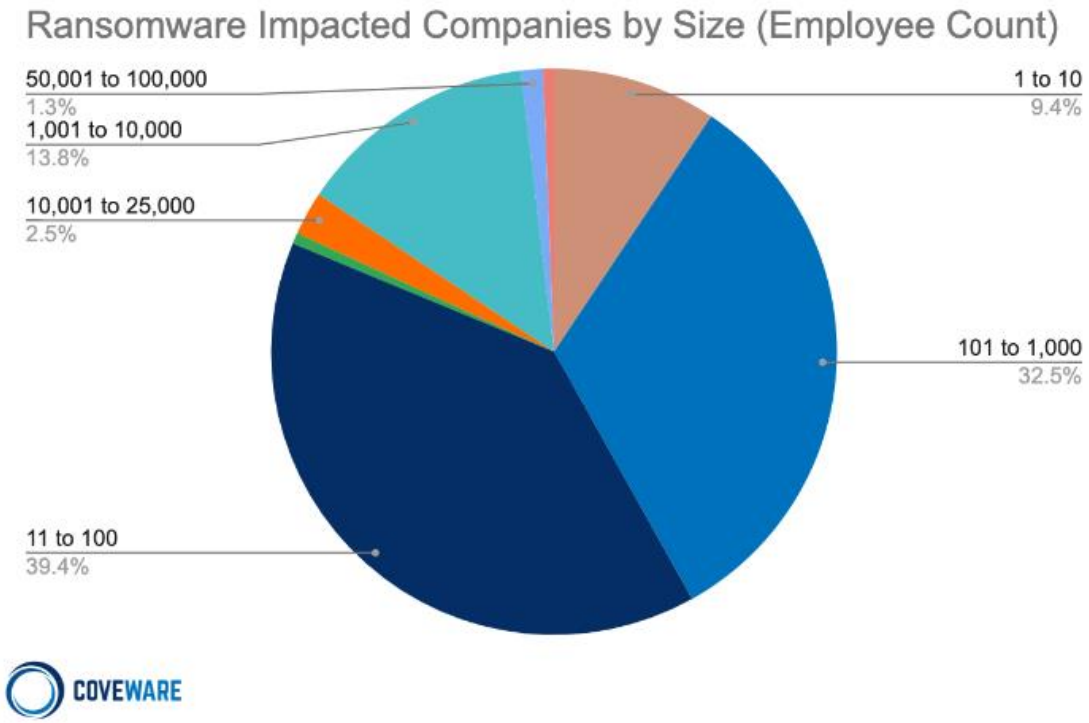
Ransomware Attacks on the Rise

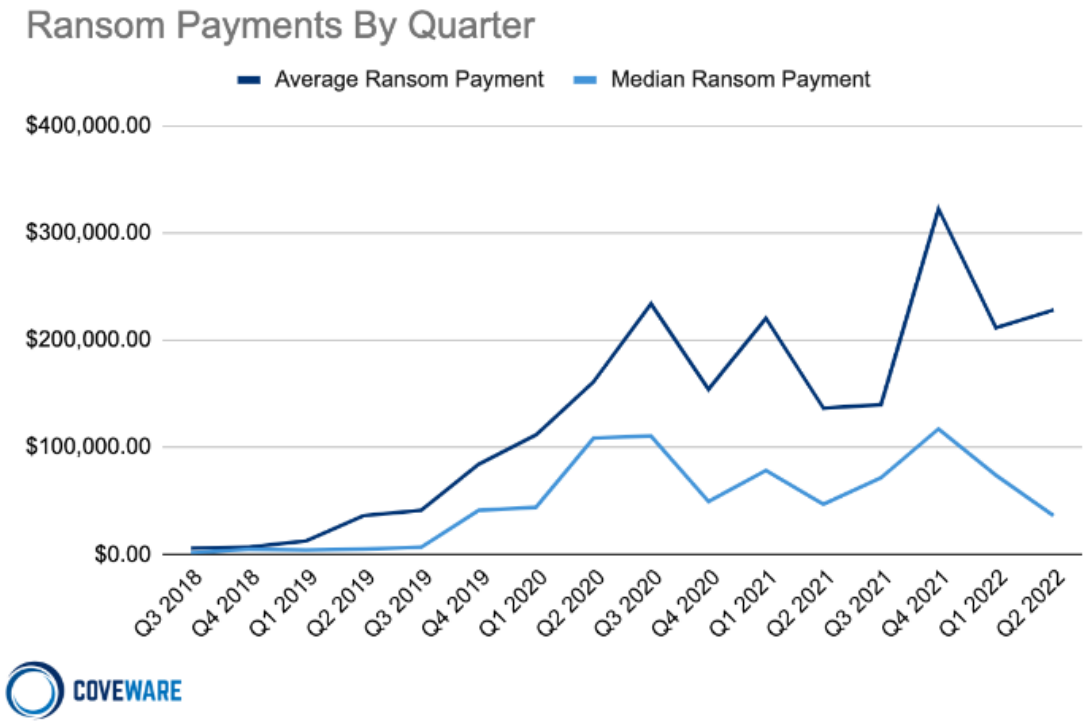


Kentucky Chamber

FORWARD
INFORMATION TECHNOLOGIES

Ransomware Attacks on the Rise





Kentucky Chamber

FORWARD
INFORMATION TECHNOLOGIES

The Uphill Battle Facing Businesses and Insurance

- Ransomware
  - Double and Triple Extortion
  - Ransomware as a Service (RaaS)
  - Think you're not a target? You're wrong.
- Business Email Compromise
- Most criminal activity is overseas, difficult to find and prosecute.
- FBI Criminal Crime Complaint Center - 2014 - 2019 Business losses jumped from $60m to $1.8b

The Cyber Liability Insurance Effect

- Cyber Liability loss ratios soared from 47% in 2019 to 73% in 2020
- Rates are rising, coverage is falling
  - A $5m policy is now a $1-$3m policy IF they will insure at all
- Insurers are demanding high-cost, disruptive (but required) solution

Recommendations

- Build the talent pipeline for cyber security workforce.
- Cybersecurity safe harbor statutes (Ohio, Utah, Connecticut)
- Avoid overly prescriptive regulations that create a patchwork of laws; focus on broad consensus on approaches at the federal level, public-private partnerships such as information sharing with government agencies, and an environment that allows the private sector to innovate.
- Increase support for law enforcement of criminals.

Kentucky Chamber

FORWARD
INFORMATION TECHNOLOGIES