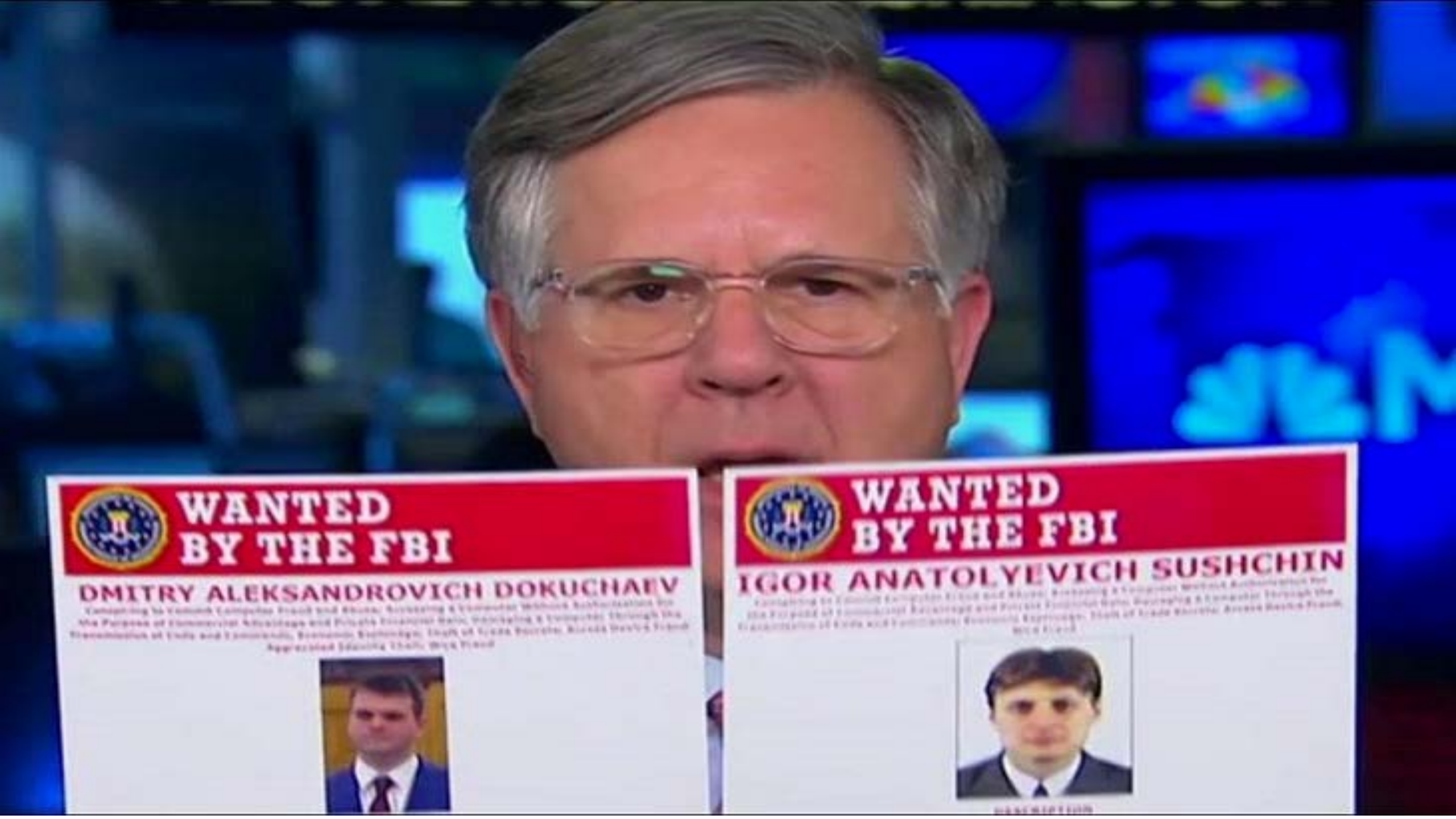
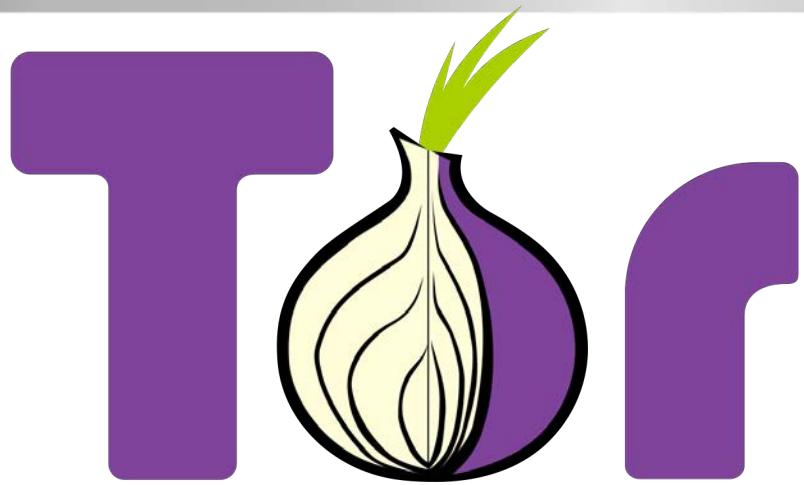
CyberDIVISION
FEDERAL BUREAU OF INVESTIGATION

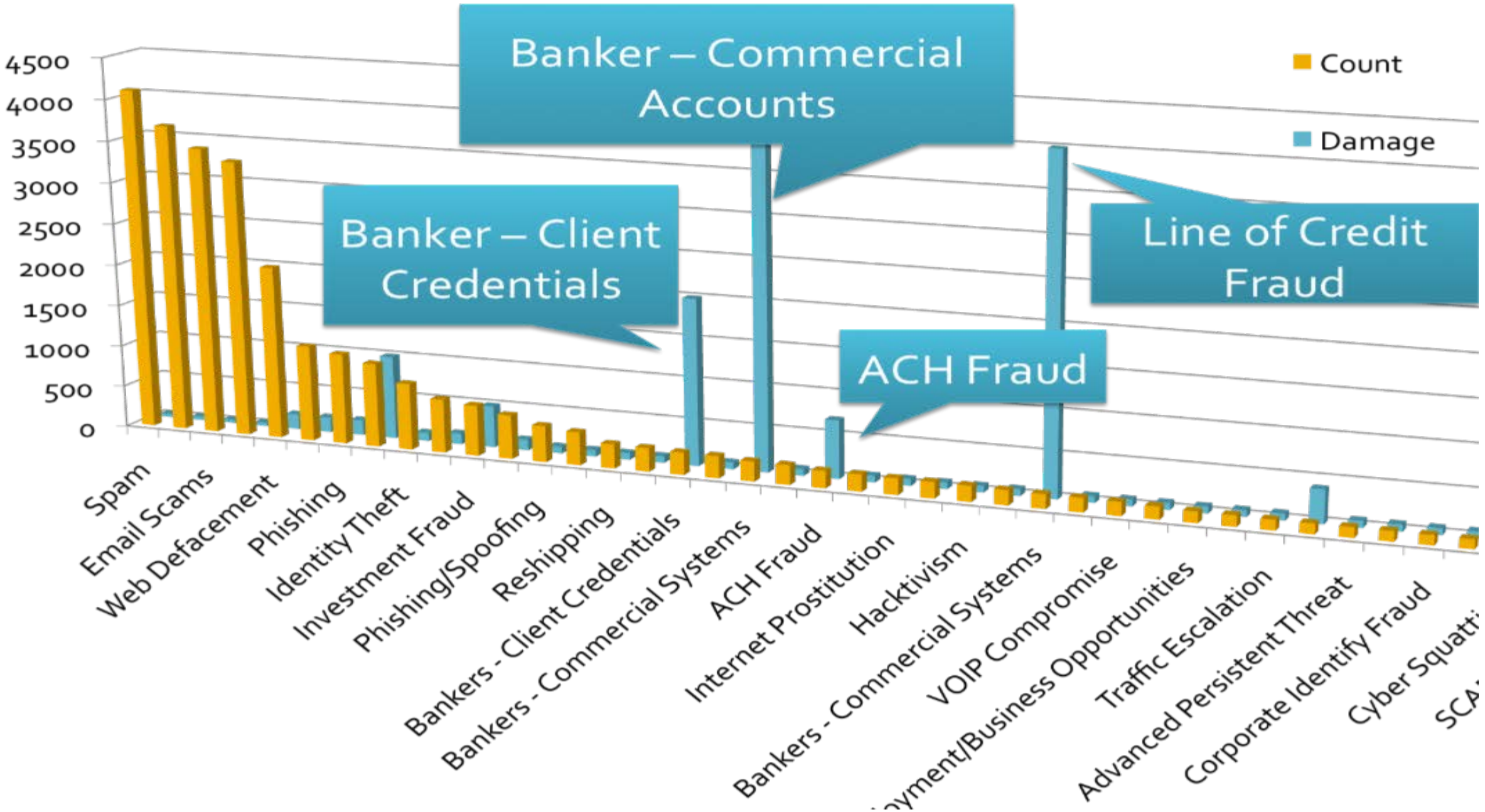
Preparing to Fail

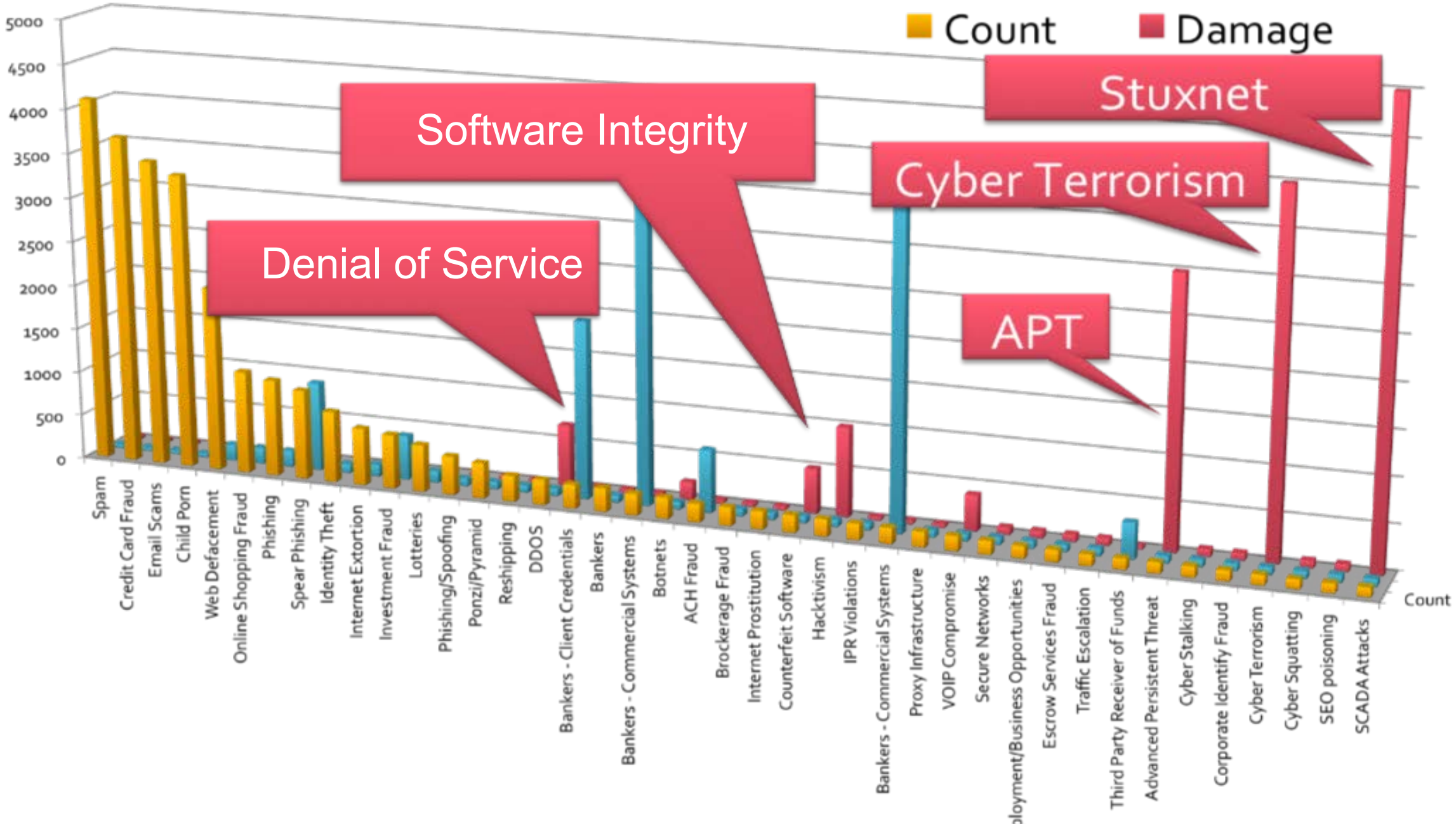
Changing the way we think about cyber threats


WANTED
BY THE FBI
DMITRY ALEKSANDROVICH DOKUCHAEV
WANTED
BY THE FBI
IGOR ANATOLYEVICH SUSHCHIN

The current state of cyber underground




Banker – Commercial Accounts
Banker – Client Credentials
ACH Fraud
Line of Credit Fraud
Count
Damage
4500
4000
3500
3000
2500
2000
1500
1000
500
0
Spam
Email Scams
Web Defacement
Phishing
Identity Theft
Investment Fraud
Phishing/Spoofng
Reshipping
Bankers - Client Credentials
Bankers - Commercial Systems
ACH Fraud
Internet Prostitution
Hacktivism
Bankers - Commercial Systems
VOIP Compromise
Traffic Escalation
Advanced Persistent Threat
Corporate Identify Fraud
Cyber Squatti


Count
Damage
Stuxnet
Software Integrity
Cyber Terrorism
Denial of Service
APT
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
Spam
Credit Card Fraud
Email Scams
Child Porn
Web Defacement
Online Shopping Fraud
Phishing
Spear Phishing
Identity Theft
Internet Extortion
Investment Fraud
Lotteries
Phishing/Spoofing
Ponzi/Pyramid
Reshipping
DDOS
Bankers - Client Credentials
Bankers
Bankers - Commercial Systems
Botnets
ACH Fraud
Brockerage Fraud
Internet Prostitution
Counterfeit Software
Hacktivism
IPR Violations
Bankers - Commercial Systems
Proxy Infrastructure
VOIP Compromise
Secure Networks
Escrow Services Fraud
Traffic Escalation
Third Party Receiver of Funds
Advanced Persistent Threat
Cyber Stalking
Corporate Identify Fraud
Cyber Terrorism
Cyber Squatting
SEO poisoning
SCADA Attacks
Count

Specific threats to the Packaging Industry

Locky

Delivered Right to Your Inbox


E-MAIL
From: Finance Director
SUBJECT: Initiate Acquisition
BANK

Primary Schemes

Name	Scheme
Supplier Swindle	The “supplier” changes receiving bank accounts
CEO Fraud	The “CEO” requests an payment for an acquisition or service
Shipping Switch-up	The “receiver” requests a change in shipping destination
3rd Party	The “3rd Party” service requests payment for services rendered
Data theft	Important data is requested for use in tax fraud

MASTERING DATA

Exclusive: Facebook and Google Were Victims of $100M Payment Scam

We must…

- Understand the threats to our company

- Design **specific** mitigation and recovery controls into our business process

Ransomware

1. Implement the technical controls within email
2. Un-flatten our networks – everyone does not need access to everything in your network
3. Back up, virtualize, and TEST recovery
4. Don’t immediately destroy the infected system
5. Explore the payment mechanism

Business email compromise

1. Implement technical controls in email such as **[external]** tags, webmail auditing
2. Two-factor authentication / Password re-use***
3. Educate the specific departments that are often targeted
   – C-Level, Finance, Human Resources, Sales, Shipping
4. Design controls that allow for failure
   –Processes for shipping, payments, acquisitions, employee information
5. Engage your 3rd parties, such as banks, consultants, law firms
6. Know who to call when failure happens, have a team in place

Other considerations

- Cyber insurance
- 3rd parties
  - Processes
  - Communication
  - Responsibilities
- Managed services
- Incident Response on retainer
- Practice responding to incidents with the entire team

Key Take Aways

- If you only remember two things from my presentation, they should be…
  1. Failure will happen
  2. Failure doesn't equal disaster, **mishandling** failure most likely will.
- When you get back to your office, the two things you should do are…
  1. Design your processes and relationships to mitigate failure
  2. **Practice your response**