ADAPT OR DIE – THE CISO’S NEW ROLE IN A SOCIAL MEDIA FIRST WORLD

EVAN BLAIR
Co-Founder
ZeroFOX
@EvanLBlair
MODERN BUSINESS LIVES OUTSIDE THE FIREWALL
Percentage of S&P 500 Market Value Comprised From Intangible Assets

17%  88%

Modern business introduces modern security risks
Where business risk and technology risk overlap has changed dramatically
We can no longer focus on technology risk in isolation from business growth and risk factors
WELCOME TO THE SOCIAL REVOLUTION
95% US working age are **active** on social media

3/4 worldwide internet users have **active** social profiles
AT THE HEART OF REAL REVOLUTIONS
27% INTERNET TIME SPENT ON SOCIAL MEDIA

3 HOURS EVERY DAY SPENT ON SOCIAL MEDIA
>52% OF ONLINE & OFFLINE PURCHASES DRIVEN BY FACEBOOK

81% OF SOCIAL MEDIA USERS PURCHASE BASED ON SOCIAL INFLUENCE
SOCIAL IS A BUSINESS PLATFORM

SOCIAL USE & INVESTMENT

83%
Global organization’s use social as key business platform

24%
of total enterprise marketing budgets spent on social in next 4 years

SOCIAL MEDIA IMPACT

40%
Outperformance in revenues / valuation vs. S&P 500

$25B
Spent on advertising products and businesses on social platforms globally
HR / Recruiting

84% of organizations are now recruiting on social media

Customer Success

70% of consumers use social networks like Twitter & Facebook for customer service

Sales

74% of salespeople who beat their quota say they use social media
SOCIAL MEDIA...
THE [MODERN] BUSINESS PLATFORM

FACEBOOK
APPLE APP STORE
GOOGLE
TWITTER
LINKEDIN
SLACK
WORKPLACE
DEEP & DARK WEB
REDDIT
PASTEBIN

...
WHERE ARE THE RISKS?

INFORMATION SECURITY
- Spoofed domains
- Targeted phishing & exploits
- Compromised credentials
- Insider, DLP & compliance

BRAND RISKS
- Brand protection
- Reputation damage
- Customer attacks
- Counterfeit & piracy

CORPORATE SECURITY
- Situational awareness
- Executive protection
- Events & travel threats
- Location protection
OLD & NEW RISKS, BUT A NEW WAY

USA TODAY
Vevo suffered a huge hack from a LinkedIn phishing scam

FORBES / Security / #CyberSecurity
Iranian Hackers Targeted Deloitte Via A Seriously Convincing Facebook Fake

The New York Times
Hackers Hide Cyberattacks in Social Media Posts
OLD RISKS, NEW COSTS

- Insurance premium increases, 2%
- Increased cost to raise debt, 4%
- Devaluation of trade name, 14%
- Lost value of customer relationships, 26%
- Operational disruption, 2%
- Incident triage, 4%
- Value of lost contract (premiums), 49%

$1.68 billion


- Breach notification
- Investigation & remediation
- Identity theft & credit monitoring
- Security improvements
- Attorney fees and litigation
- Regulatory fines (HIPAA)
WHAT DO WE HAVE TO LOSE?

BRANDZ™ STRONG BRANDS PORTFOLIO VS. S&P 500 VS. MSCI WORLD INDEX

The value of the BrandZ™ Strong Brands Portfolio increased 124.9 percent between April 2006 and April 2017, outperforming both the S&P 500 and the MSCI World Index.

Source: Kantar Millward Brown / BrandZ™
The BrandZ™ Strong Brands Portfolio is a subset of the BrandZ™ Top 100 Most Valuable Global Brands.
Percentage of S&P 500 Market Value Comprised From Intangible Assets

17%  88%

UNPACKING THE REAL VALUE OF YOUR ASSETS

WHAT REALLY ARE YOUR INTANGIBLE ASSETS?

RIGHTS
- Licensing, royalty, & service agreements
- Financing terms
- Supply contracts & franchises
- Usage rights (e.g., drilling, water, air, mineral, timber, etc.)

RELATIONSHIPS
- Customer relationships (non-contractual)
- Production & distribution channels
- Alliances & joint ventures
- Corporate reputation & culture

IP
- Trademarks & tradenames
- Patents & copyrights
- Trade secrets & knowhow
- Customer lists
- Proprietary technology
// JUST LOOK AT FACEBOOK
DON’T FORGET ABOUT GDPR!
A COMPOUNDING PROBLEM

Ransoc Desktop Locker Ransomware Scans Social Media Profiles for Exploitation

AdultFriendFinder network hack exposes 412 million accounts

Cyber security experts warn firms about hacker

Mark Zuckerberg Hacked

Sir Patrick Stewart's Twitter hacked by PORN bot which posted X-rated images on his account

Promoted Tweet leads to credit card phishing

Drug sales on social media security expert says

Facebook Sees 600,000 Compromised Logins Per Day

Confidential & Proprietary
<table>
<thead>
<tr>
<th>TARGET</th>
<th>WHY / IMPACT</th>
<th>TACTICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMPLOYEES</td>
<td>Humans are compromised in order to <strong>bypass security defenses</strong> and gain access to “protected” systems and sensitive data</td>
<td>HASHTAG HIJACKING, ACCOUNT TAKEOVER</td>
</tr>
<tr>
<td>BUSINESS ASSETS</td>
<td><strong>Sensitive, confidential &amp; protected information is published</strong> &amp; malicious actions coordinated to damage revenue generating activities &amp; biz trust</td>
<td>IMPERSONATIONS, ATTACK PLANNING, SOCIAL PHISHING, SOCIAL ENGINEERING</td>
</tr>
<tr>
<td>CUSTOMERS</td>
<td><strong>Customers are targeted through fraudulent impersonations</strong> of the org and key executives to steal customer data &amp; damage reputation</td>
<td>INFORMATION LEAKAGE</td>
</tr>
</tbody>
</table>
TRADITIONAL NETWORK ATTACK VS. SOCIAL ATTACK

TRADITIONAL NETWORK ATTACK

STEP 1: Footprinting Whois, DNS
STEP 2: Scanning, Ping, Portscan
STEP 3: Enumeration Vuln Scans
STEP 4: Exploit Attacks

Vulnerable
Firewall detection occurs early in attack lifecycle
Build a network of “trust”!!!
QUICK EXAMPLE
IN THE WILD

THREAT: SPOOFED ACCOUNTS
THREAT: SPOOFED ACCOUNTS

BY THE NUMBERS

- Pretend to be someone/thing else
- 11X increase over 2 years
- 38% redirect to phishing pages
- Paid social promotion, verification
- Other examples:
  - Financial scams
  - Counterfeit offers
  - Fake job recruiters

FIGURE 1
Pie chart illustrating the breakdown of total impersonations per social network. Pie segments display absolute number of impersonations next to the relative percentage of total impersonations across social networks.
IN THE WILD

THREAT: SOCIAL PHISHING

@PayPal is a joke stopping me from using my PayPal account till i send of a bank statement well i am raging 😡😡😡

PayPal
@AskPayPal_Tech

Hi [redacted], We sincerely apologize for this. In order to regain access to your account, Please visit bit.ly/[redacted]Lxs7

3:11 PM - 19 Aug 2016
THREAT: SOCIAL PHISHING

IN THE WILD

REAL

THREAT: SOCIAL PHISHING
THREAT: SOCIAL PHISHING

SCALE
Facebook is the most common delivery mechanism for malware; the #1 way to breach the network
- CISCO

FREQUENCY
7.57 million victims annually
- Kaspersky

IMPACT
Avg enterprise company spends $3.7M / year remediating phishing
- Kaspersky & CSO Magazine

WHO?
92% of employees have experienced cyberattacks on social
- Barracuda
IN THE WILD

THREAT: ACCOUNT TAKEOVER
Adaptation.

ADAPT (or die, aka APPLY)
WHO IS A [MODERN] CISO?
87% Of global security workforce did not start in cyber

43% Of global security C-suite from non-security & non-technical background
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Alignment with business leaders</td>
</tr>
<tr>
<td>2.</td>
<td>Understanding of balance between business &amp; technology risk</td>
</tr>
<tr>
<td>3.</td>
<td>A focus on building cross-functional teams</td>
</tr>
<tr>
<td>4.</td>
<td>Defined communication plan that is frequent and bi-directional</td>
</tr>
<tr>
<td>5.</td>
<td>Hiring program that looks for diverse backgrounds</td>
</tr>
<tr>
<td>6.</td>
<td>Focus on workforce improvement and skill building, enhancing existing diverse perspectives</td>
</tr>
<tr>
<td>7.</td>
<td>Created culture of value protection vs. risk mitigation</td>
</tr>
</tbody>
</table>
HOW TO BECOME A MODERN CISO

1. Understand *how* the business grows
   1. Schedule 1-on-1 meetings with executive / leadership peers
2. Engage with your Organization: Communication is Key
   1. Communicate business first security strategy and explain asks from business leaders & employees
3. Establish cross-functional “working group” to support business & technical risk alignment
4. Inventory *external* technologies in use across the organization
   1. Work with business units & ensure your engagement is NOT confrontational or “security” focused
5. Identify high-impact *external* risk events
   1. This should stem from your understanding of how the business grows – not all risk events have same impact on different businesses
6. Create shared departmental responsibility and process for addressing *external* risk events
7. Integrate technology
8. Communicate
9. Go Back to #1
THANK YOU!

Evan Blair
Co-Founder, ZeroFOX

@EvanLBlair

855-ZFOX-FOX

1834 South Charles Street
Baltimore, MD 21230