

[I. OVERVIEW]

[Context] is imp't in forensics.

Without [knowing what could happen] \rightarrow \nrightarrow context \rightarrow \nrightarrow forensics

businesses & orgs
rely on tech
(ex., PoS systems)

cyber risks continue
 \uparrow to expand & influence
other types of vics

(possible) \downarrow
Importance of Cyber Risk Governance

some are essentially
"tech companies"
(to keep up w/ demands in
evolving competitive landscape)

ex., tech involved in processes (supply chain,
manufacturing, etc.) of (not necessarily tech)
products such as handbags

② Stealth

- * malware files encrypted & camouflaged
to blend w/ other legit sys. files
- \Rightarrow \nrightarrow distinguish from parts of OS

③ Wipeout Techniques

- * anti-forensic techniques to reliably
erase traces of own activity
- \Rightarrow make retracing & understanding
actions more difficult

④ Hijacking

- * hijack legit software to manipulate its logic

Escalation of ransomware

INET Iter.
Targeted at indivs;
revenue: "retail victims"

NEXT Iter.
Targeted at corps;
revenue: data decryption

CURRENT Iter.
Targeted at corps (often via
supply chain);
revenue: reputation &
business preservation

① Obfuscation

- * use of protection & obfuscation
that is notoriously difficult to
break
- * protection software hides
intellectual props. contained in
legit. commercial software

Cyber Atk Techniques

more frequent
data breaches

global supply
chain threat

more disruptive attks
against cloud

biometric data more
valuable to threat actors

SG Cyber Trends

\rightarrow AI: double-edged sword!
 \rightarrow risk towards smart
buildings & connected sys. \uparrow

⑤ Surveillance

- * deploy malicious modules to record frames (i.e., screenshots) &
keystrokes \rightarrow reassemble into viewable recordings
- * used to fully understand workings of sys before attempting to
subvert it

⑥ Watering Holes

- * masquerade as "legit website" to bait victim of interest before engaging

⑦ Exploits

- * find & exploit "holes" in system
- * ASYMMETRIC DEFENDER ATTACKER PARADOX:
attacker only needs 1 hole to get in, but defender needs to fix all holes to be secure

⑧ False Flags

- * malware authors place false flags w/in their tools to stall/confuse investigators
- ex., diversionary language codes & various incorrectly transliterated words to
mislead research into true identity of attackers

⑨ Anonymity

- * set up proxies b/wn themselves & end target \rightarrow long chain for investigators to trace

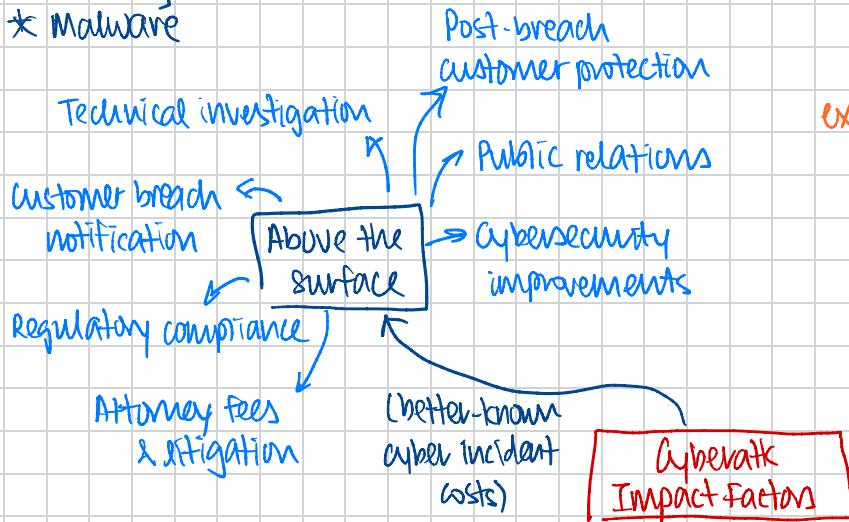
Change in Attel's Approach

- ① attack shifting from tech → p/m
 - ② attack patterns hiding in plain sight
 - ③ attackers building widening capability gaps
 - ④ supply chain & business partner sabotage ↑
 - ⑤ advanced threats defying traditional detection mechanisms

An attack scheme can involve multiple attack types.

Cyber Threats in Focus

- * Advanced Persistent Threats (APTs)
 - * Scams
 - * Phishing
 - * Malware



Malware

Programs that perform unwanted actions on computers (ex., steal personal info); possible artifacts:
→ virus, trojan, rootkit, worm, bot, ransomware

used to extort \$ from victims; may restrict access to data by encrypting files or locking computer screens

Common Cyber Atk Types

Phishing

attempt to acquire info (ex., credentials, credit card info) by posing as a trusted source in an electronic communication
ex., deceptive emails, malware, compromised networks, malicious websites

le (MITM)

Act of eavesdropping on commun. b/wn 2 parties online ; info then used to intercept & go-betw bn parties in conversation

(ex, unknown Wi-Fi networks, man-in-the-browser, man-in-the-email)

Dumpster Diving

obtaining sensitive info that is discarded carelessly; can be used to fake legitimacy

Social Engineering

Art of gaining access to buildings, sys.,
or data by exploiting human psychology,
rather than by breaking in or using technical
hacking techniques

Cybersecurity Impact Factors

