AI & Cybersecurity Newsletter

January 2022

Highlights

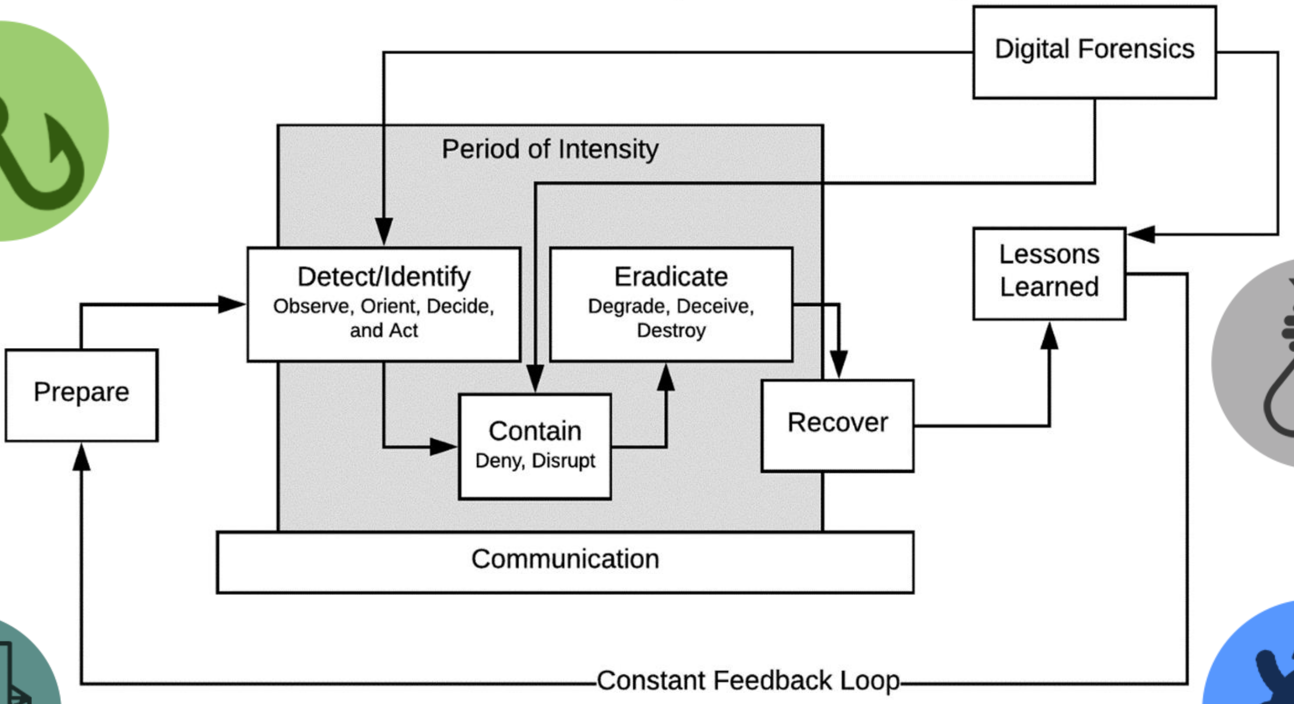
Modern Cyber Attack Incident Response Life Cycle

Cognitive Bias & Cybersecurity – Mosquito versus Shark

Survey: 1/3 Respondents Experienced $100k+ Breach in Last 12 Months

Upcoming Conferences

Modern Incident Response Life Cycle



https://sbscyber.com/resources/top-5-most-common-incident-response-scenarios

> “Amateurs hack systems,
>
> professionals hack people.”
>
> ~Bruce Schneier

Cognitive Bias & Cybersecurity - Mosquito versus Shark

Cybersecurity is a people problem, driven by our perception of risk. Tools help. In fact, tools are incredibly necessary but tools are also only as good as the people implementing them. Also, the work culture has a huge impact on behavior because employees tend to gravity toward the middle of the group, modeling their behavior to fit in, and be accepted as part of the team – for better or worse from a security best practices standpoint.

67% of security breaches are due to human behavior, not the failure of tools.

People have to digest a lot of information and success often means navigating that information efficiently, making decisions quickly – like to avoid getting in an accident on the freeway. But, that quick decision-making is not helpful during a cyberattack. People have unconscious biases that often serve them well in the workplace in general but can be catastrophic when exploited by a hacker.

Cognitive bias – There are so many categories of cognitive bias, each defined and labeled differently by the experts. Rather than try to examine and exhaust each, i.e. more information overload, here are 10 types of cognitive bias:

1) Anchoring – I looked at some of the information and my mind is made up.

2) Confirmation bias – The opposite of anchoring – I know what I will find, if I look. Oh, there, I looked and yep, I found what I was expecting to find.
3) Herd behavior – That person is not concerned about changing their password and they have never been hacked, so why should I go to the trouble?
4) Choice/Decision fatigue – There are so many cybersecurity tools available, which one is best? Do I need another? Plus, a constant barrage of work, meetings, information, alerts, tools and I don't know where to start. So, I will play wordle instead.
5) Optimism bias – I put security protocols in place and I hired good people, my job is done.
6) User Fatigue – I have followed all the rules and now you want me to update my whatever again, I am tired of updating and I work too much to have to worry about this again.
7) Alert Fatigue - Too many false positives lead even the most conscientious employees to start ignoring all alerts.
8) Ostrich approach – Head down on my work, not on security. La la la… What security issue, I cannot hear you!
9) Placebo effect – I put security practices in place when I started the company. I am covered.
10) Parkinson's Law of Triviality (Bikeshedding) – Employees often deal with a lot of trivial tasks and not enough time on the big impact items as it relates to overall corporate security. Sometimes this is due to the complexity of security issues. People gravitate toward doing what they know versus spending the time to learn the more difficult parts.

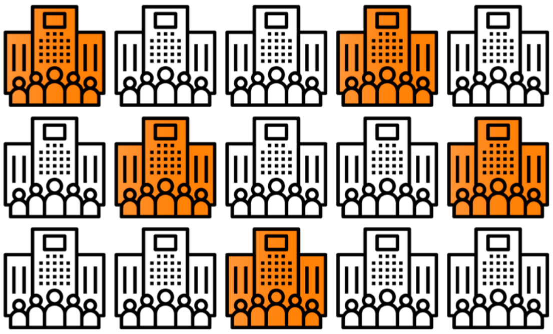
You can observe cognitive bias play out in real-time on Facebook. Either a person has friends who agree with them 100% of the time or the dissenter is mocked and blocked. That person's page becomes an echo chamber where they only hear opinions that precisely match their own. Therefore, they must be correct. Others allow a "troll" to attack and berate a topic they care very much about and the user becomes depressed and despondent that the entire world has gone mad, is uncaring, and resolving this issue is beyond hope. All is lost.

Information is not only as good as the source; it is as good as the user. Are you afraid of a shark or a mosquitos. I say shark! But, mosquitos kill more people each day than sharks kill in 100 years. Interesting point… Of course, head to head, I think I might be able to take the mosquito, not the shark. Education, training, and explaining cognitive bias to everyone in the organization makes all those cybersecurity tools much more valuable.

Key results from an Arctic Wolf survey of 1400 IT decision makers in the US, UK, and Canada

One third of respondents experienced a six-figure security breach in the last 12 months. 21% stated they concealed a cyber-attack to preserve the reputation of their business. 61% of business owners admitted concealing a breach themselves.

They see China and Russia as the most dangerous threats to the security of their businesses. They do not believe diplomacy is effective in stopping future attacks. 31% believe retaliation is effective.

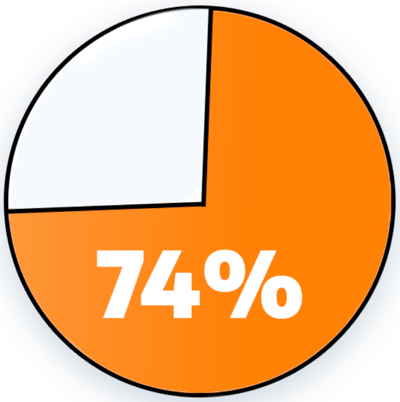


1 IN 3

ENTERPRISES

experienced a six-figure breach in the past twelve months

While 55% of these companies plan on hybrid work, most (74%) of them do not believe they have the capability to expertise to prevent cyberattacks under this work approach. 60% of respondents believe their employees could not identify an attack targeting their business.



OF EXECUTIVES

believe their in-house I.T. and security teams lack in capability and expertise

60% also believe new tools and services are the most effective way to prevent attacks.

Conferences

January 23	Ransomware Resilience & Recovery, Virtual
January 26-28	SNIA 2021 Annual Members Symposium, Virtual
January 27- Feb 5	Cyber Threat Intelligence Summit & Training, Bethesda
February 2-4	IT DEFENSE 2022, Berlin
February 7-11	Cisco Live, Amsterdam
February 8-11	ITExpo, Fort Lauderdale
February 14-15	Gartner Security & Risk Management Summit, Dubai
February 17-18	Deep Learning Hybrid Summit, San Fran & Virtual
February 28- March 3	MWC Barcelona
March 2-3	Big Data & AI World, London
March 2-3	Cloud Expo Europe, London
March 2-3	Cloud & Cyber Security Expo, London
March 11-12	SXSW 2022, Austin
March 14-16	Gartner Identity & Access Management, Vegas
March 14-17	Gartner Data & Analytics Summit, Orlando
March 23-24	Paubox SECURE 2022, Vegas
March 28-31	Data Center World, Austin
April 19-21	ODSC East, Boston
April 23-27	NAB, Vegas
April 26-28	Smart NICs Summit, San Jose
May 4-5	World Summit AI Americas, Montreal
May 9-11	Gartner Data & Analytics Summit, London
May 10-13	Black Hat Asia, Singapore

May 11-12	AI & Big Data Expo, Santa Clara
May 11-12	Cyber Security & Cloud Congress, Santa Clara
May 18-19	Gartner Digital Workplace Summit, London
June 6-9	RSA Conference, San Francisco & Virtual
June 7-10	Women in Tech Global Conference 2022, TBA & Virtual
June 12-16	Cisco Live, Vegas
June 14-16	Digital Enterprise Show, Malaga
June 15	Cloud Security Summit, Virtual
June 21-22	Gartner Security & Risk Management Summit, Sydney
June 21-22	Gartner Digital Workplace Summit, San Diego
June 29- July1	Mobile World Congress, Shanghai
July 19-20	Cyber Solutions Summit & Expo, Virtual
August 2-4	Flash Memory Summit, Santa Clara
August 6-11	Black Hat USA, Vegas
August 11-14	DEF CON 30, Vegas
September 13-14	CISO Forum, Virtual
September 19-20	Industry of Things World, Berlin
September 28-29	IoT World, Santa Clara
October 5-6	Evolve, Vegas
October 24-27	ICS Cybersecurity Conference, Hybrid/Virtual
November 16	San Diego Cybersecurity Conference, Hybrid
November 16	Threat Hunting Summit, Virtual
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
December 1-2	AI & Big Data Expo Global, London
December 6	Security Operations Summit, Virtual