Highlights

“The Executives need to be able to consume the complexities of cyber-risk in business terms and receive repeatable, meaningful metrics upon which to base risk decisions. Often, the information being provided by CISOs and security teams to update management on their cyber exposure is highly complex and generated in a technical lexicon. This thwarts the ability of management to truly understand much less calculate value regarding cyber-risk, and ultimately puts them at a disadvantage regarding their ability to effectively prioritize, govern, and execute on cyber programs that can have operational, financial, and reputational impacts…

Balance sheets, and financial statements in general, exist to provide a broad view of the financial performance of an entity. They are based on a standard framework that takes vast amounts of data from many different sources and systems and consolidates that information down to a cohesive view of financial performance that is easily understood by those who consume it. The demands of cyber-risk reporting are analogous; large amounts of technical risk data need to be consumed from many systems and synthesized down to easily understandable, meaningful business risk terms to allow a variety of stakeholders to make decisions.

Andrew Morrison, Principal, Cyber Risk Services, Deloitte Advisory

Navy Must Move From Compliance to Readiness Approach to Cybersecurity

"We view cybersecurity as a compliance problem. And it is most definitely not a compliance problem," Navy Chief Information Officer Aaron Weis said, arguing they must shift to a "readiness" focus. “Today, I would argue that the way that we do cybersecurity at the Department of Navy- and at the Department of Defense but that’s above my paygrade- … is wrong,” Cybersecurity through compliance results in risk increases, delayed capabilities, inadequate protection and wasted resources, according to Weis. Instead, the service needs to move toward a readiness model that is measured holistically, he said. “And when I talk about readiness, I’m not saying it’s fleet readiness … I’m saying it’s a model inspired by how we approach readiness,” Aaron Weis, Navy CIO, said. “Readiness is something that is a dynamic model … It is measured very holistically.” The Navy has been working towards its new, holistic model since last November and to that end created a program called Cyber Ready. With the program, the service wants to shift cybersecurity away from rote compliance bureaucracy and towards a “cyber ready” state that enables acquisition speed and better defends the service’s information.
“I’m of the mind that cyber is probably one of the most overused words in this town, in this industry … It means everything to everyone,” he said. “And, therefore, it sort of means nothing. So, we have to put a finer point on it. We have to defend our information wherever it lives — at rest, in transit, in the industrial base, in our systems, at the tactical edge. You name it, we have to be able to defend it.”

“Shared Interest” Technique to Determine When AI Models Hits and Misses the Target

In machine learning, understanding why a model makes certain decisions is often just as important as whether those decisions are correct. While tools exist to help experts make sense of a model’s reasoning, often these methods only provide insights on one decision at a time, and each must be manually evaluated. Models are commonly trained using millions of data inputs, making it almost impossible for a human to evaluate enough decisions to identify patterns.

Researchers at MIT and IBM Research have created a method called Shared Interest to enable a user to aggregate, sort, and rank these individual explanations to rapidly analyze a machine-learning model’s behavior. The technique incorporates quantifiable metrics that compare how well a model’s reasoning matches that of a human. Aggregating insights can help the user quickly and quantitatively determine whether a model is trustworthy and ready to be deployed in a real-world situation.

Shared Interest leverages popular techniques that show how a machine-learning model made a specific decision, known as saliency methods. If the model is classifying images, saliency methods highlight areas of an image that are important to the model when it made its decision. These areas are visualized as a type of heatmap, called a saliency map, that is often overlaid on the original image. If the model classified the image as a dog, and the dog’s head is highlighted, that means those pixels were important to the model when it decided the image contains a dog. When evaluating an image classification model, Shared Interest compares the model-generated saliency data and the human-generated ground-truth data for the same image to see how well they align.

The technique uses several metrics to quantify that alignment (or misalignment) and then sorts a particular decision into one of eight categories. The categories run the gamut from

perfectly human-aligned (the model makes a correct prediction and the highlighted area in the saliency map is identical to the human-generated box) to completely distracted (the model makes an incorrect prediction and does not use any image features found in the human-generated box).

“On one end of the spectrum, your model made the decision for the exact same reason a human did, and on the other end of the spectrum, your model and the human are making this decision for totally different reasons. By quantifying that for all the images in your dataset, you can use that quantification to sort through them,” doctoral student Angie Boggust explains.

In one case study, Shared Interest was employed by a dermatologist to determine if he should trust a machine-learning model designed to help diagnose cancer from photos of skin lesions. Shared Interest enabled the dermatologist to quickly see examples of the model’s correct and incorrect predictions. Ultimately, the dermatologist decided he could not trust the model because it made too many predictions based on image artifacts, rather than actual lesions.

“The value here is that using Shared Interest, we are able to see these patterns emerge in our model’s behavior. In about half an hour, the dermatologist was able to make a confident decision of whether or not to trust the model and whether or not to deploy it,” Boggust says.

Their technique enables researchers to analyze thousands of correct and incorrect decisions in a fraction of the time required by typical manual methods.

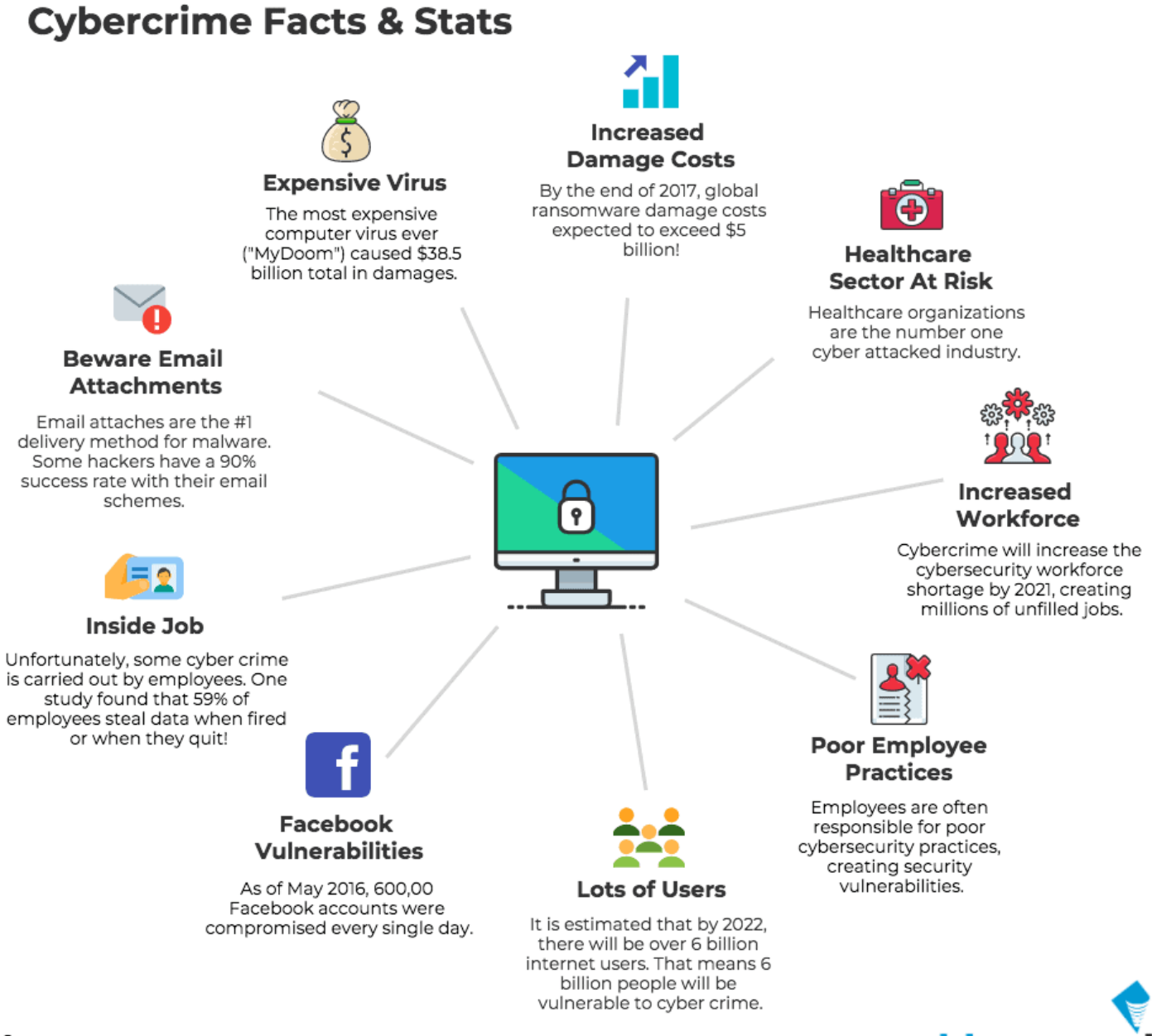
CISA Catalog of Bad Practices

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA is developing a catalog of Bad Practices that are exceptionally risky, especially in organizations supporting Critical Infrastructure or NCFs. The presence of these Bad Practices in organizations that support Critical Infrastructure or NCFs is exceptionally dangerous and increases risk to our critical infrastructure, on which we rely for national security, economic stability, and life, health, and safety of the public. Entries in the catalog will be listed here as they are added.

1. Use of unsupported (or end-of-life) software in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.

2. Use of known/fixed/default passwords and credentials in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
3. The use of single-factor authentication for remote or administrative access to systems supporting the operation of Critical Infrastructure and National Critical Functions (NCF) is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.



Sources:
http://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/
https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
https://www.darkreading.com/endpoint/5-reasons-cybercriminals-target-healthcare/d/d-id/1325210?
https://www.optus.com.au/enterprise/accelerate/security/10-sobering-facts-and-stats-about-cyber-crime
https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/

blue-pencil
Information Security
@BluePencil_Info

Bug Bounty Programs – Get Paid to Make Others More Secure

Bug Bounty Programs

1) Apache

Minimum payout: $500

Maximum Payout: $3000

2) Apple

Minimum Payout: No minimum

Maximum payout: $100,000 to those who can extract data protected by Apple's Secure Enclave technology, $200,000 for security issues affecting its firmware.

3) AT&T

Minimum Payout: $500

Maximum Payout: No maximum

4) Avast

Minimum Payout: $400

Maximum Payout: $10,000.

5) Bugcrowd

A powerful platform connecting the global security researcher community to the security market. This site aims to provide right mix and type of researcher suited according to the specific website to their worldwide clients. The hackers just need to select their reports on this site, and if they can detect right bugs, the specific company will pay the amount to that person.

6) Cisco

Minimum Payout: $100

Maximum Payout: $2,500

7) Dropbox

Dropbox bounty program allows security researchers to report bugs and vulnerabilities on the third-party service HackerOne.

Minimum Payout: $12,167

Maximum Payout: $32,768

8) Facebook

Under Facebook's bug bounty program users can report a security issue on Facebook, Instagram, Atlas, WhatsApp, etc.

Minimum Payout: $500

Maximum Payout: No maximum

9) GitHub

Minimum Payout: $200

Maximum Payout: $10,000

10) Google

Every content in the .google.com, .blogger, youtube.com are open for Google's vulnerability rewards program.

Limitations: This bounty program only covers design and implementation issues.

Minimum Payout: $300

Maximum Payout: $31.337

11) HackerOne

HackerOne is one of the biggest vulnerability coordination and bug bounty platform. It helps companies to protect their consumer data by working with the global research community for finding most relevant security issues. Many known companies like Yahoo, Shopify, PHP, Google, Snapchat, and Wink are taking the service of this website to give a reward to security researchers and ethical hackers.

12) Intel

Intel's bounty program mainly targets the company's hardware, firmware, and software.

Limitations: It does not include recent acquisitions, the company's web infrastructure, third-party products, or anything relating to McAfee.

Minimum Payout: $500

Maximum Payout: $30,000

13) LinkedIn

Minimum Payout: No minimum

Maximum Payout: No maximum

14) Magento

Limitations:

Following security research is not eligible for the bounty- Potential or actual denial of service of Magento applications and systems, Use of an exploit to view data without authorization, Automated/scripted testing of web forms

Minimum Payout: $100

Maximum Payout: $10,000

15) Microsoft

Limitations: The bounty reward is only given for the critical and important vulnerabilities.

Minimum Payout: $15,000 for finding critical bugs (recent news indicate changes/increases in bounties, there are many bounty opportunities)

Maximum Payout: $250,000

16) Mozilla

Limitations: The bounty is offered only for bugs in Mozilla services, such as Firefox, Thunderbird and other related applications and services.

Minimum Payout: $500

Maximum Payout: $5000

17) OpenSSL

OpenSSL bounty allows you to report vulnerabilities using secure email (PGP Key). You can also report vulnerabilities to the OpenSSL Management Committee.

Minimum Payout: $500

Maximum Payout: $5000

18) Paypal

Payment gateway service Paypal also offers bug bounty programs for security researchers.

Limitations:

Vulnerabilities dependent upon social engineering techniques, Host Header

Denial of service (DOS), User defined payload, Content spoofing without embedded links/HTM and Vulnerabilities which require a jailbroken mobile device, etc.

Minimum Payout: $50

Maximum Payout: $10,000

19) Paytm

Limitations: Reports that state that software is out of date/vulnerable without a ‘Proof of Concept’, XSS issues that affect only outdated browsers, Stack traces that disclose information, Any fraud issues

Minimum Payout: $15

Maximum Payout: No maximum

20) Perl

Minimum Payout: $500

Maximum Payout: The highest amount given by Perl is $1500.

21) PHP

PHP allows ethical hackers to find a bug in their site.

Maximum Payout: $500

Minimum Payout: $1500

22) Quora

Minimum Payout: $100

Maximum Payout: $7000

23) Shopify

Minimum Payout: $500

Maximum Payout: There is no fix upper limit for paying the bounty.

24) Snapchat

Minimum Payout: $2000

Maximum Payout: $15,000.

25) Starbucks

Minimum Payout: $100

Maximum Payout: $4000

26) Tor Project

Tor Project's bug bounty program covers two of its core services: its network daemon and browser.

Limitation: OpenSSL applications are excluded from this scope.

Minimum Payout: $100

Maximum Payout: $4000

27) Twitter

Minimum Payout: $140

Maximum Payout: $15,000

28) Uber

Minimum Payout: No minimum

Maximum Payout: $10,000 for finding critical bug issues.

29) Vimeo

Minimum payout: $500

Maximum Payout: $5000

30) WordPress

Minimum Payout: $150

Maximum Payout: No maximum

31) Yahoo

Limitations: The Company does not offer any reward for finding bugs in yahoo.net, Yahoo 7 Yahoo Japan, Onwander and Yahoo operated WordPress blogs.

Minimum Payout: No minimum

Maximum Payout: $15,000

32) Zomato

Minimum Payout: $1000

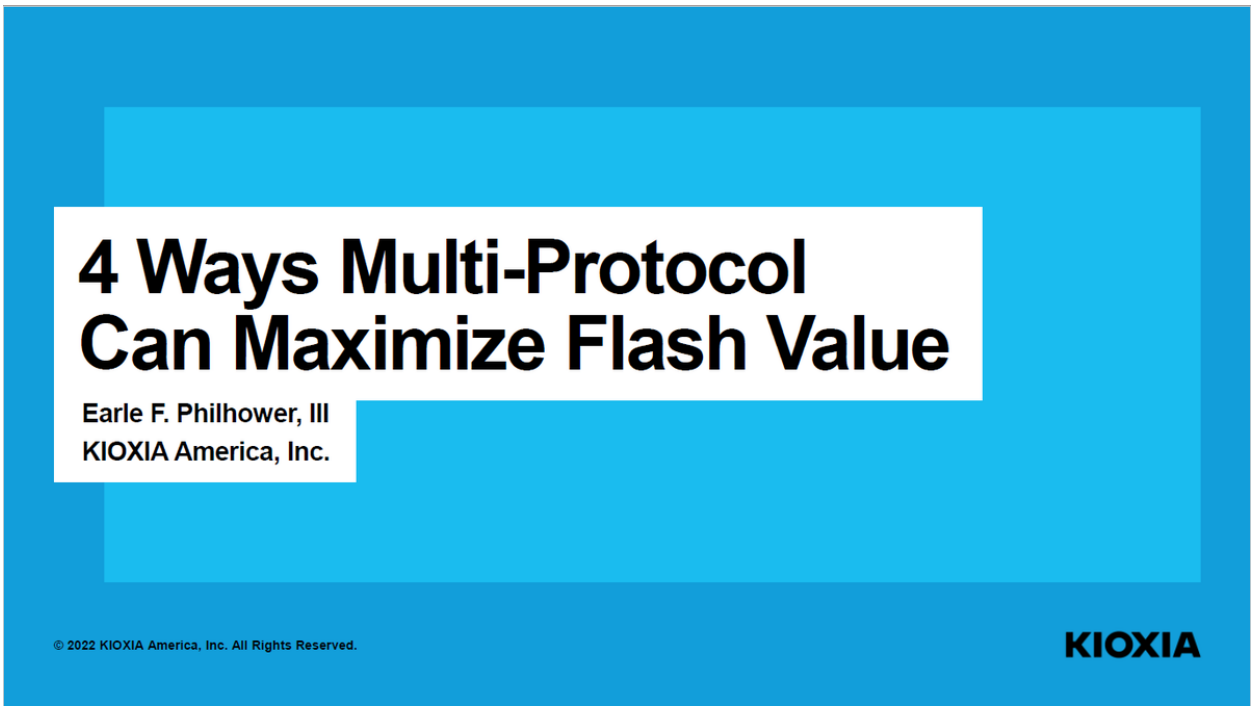
Maximum Payout: No maximum

KIOXIA Webinar Series

Wednesday, March 30, KIOXIA presented “Large-Scale Data Center Revolution for Flash Storage.” Large-scale data centers present unique challenges for the optimal use of flash storage. Problems such as "noisy neighbors", data placement, and the widely varying latency requirements of different classes of applications are incredibly difficult to solve simultaneously with conventional flash architectures. Software-enabled flash (SEF) provides a means to effectively address the challenges of cloud data center. Find out how KIOXIA is approaching these issues with its market-leading approach to SEF by viewing the webinar here and the slidedeck is available here.

Tuesday, February 8, KIOXIA provided an analysis of “4 Ways Multi-Protocol Can Maximize Flash Value.” The webinar video is available to view here and the slidedeck is available here.
Each webinar stands alone and collectively provides an overview of the innovation, direction, and leadership KIOXIA provides in this enterprise storage space.

November 17, KIOXIA presented the second webinar in their four-part webinar series, “The Next Flash Revolution at Scale: Open Source Software + Software-Enabled Technology.” The video is available to view and a copy of the slidedeck is available here. KIOXIA webinar Part 1, “Why Flash Memory At Scale Should be Software-Defined” is available to view here along a copy of the slidedeck here.



Upcoming Conferences

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