RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **EZCL-T02**

You already have the data, now use it to measure your people-centric risk

Masha Sedova

Co-founder, Chief Product Officer
Elevate Security
@modMasha

Elevate Security

Why do we need to measure human-centric risk?

You can’t change what you can’t see

Are your interventions *working*?

What does you need to focus on?

When are you *done*?

Why we measure

- For the same reasons we measure anything else:

  To know what it is

  To know how it works

  To know how to manage it

- Measurement allows us to know if security is effective.
- Appropriately prioritize our resources
- Measurement shows us the impact of security decisions
- Measurement helps us communicate to others
- Understand our security strengths and weaknesses

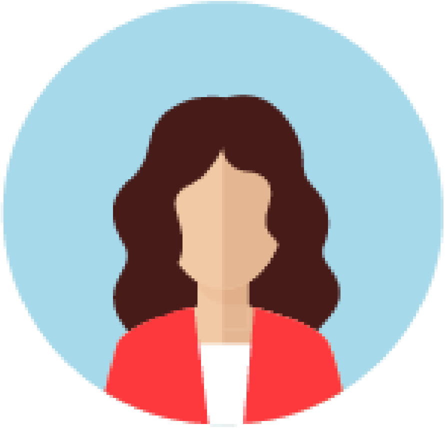
“Organizations that base security awareness on measurable learning outcomes will experience **40% fewer user-generated security incidents** than organizations that maintain traditional awareness programs.”

-Gartner Report

What should we be measuring?

Different security thumbprints, but same training?

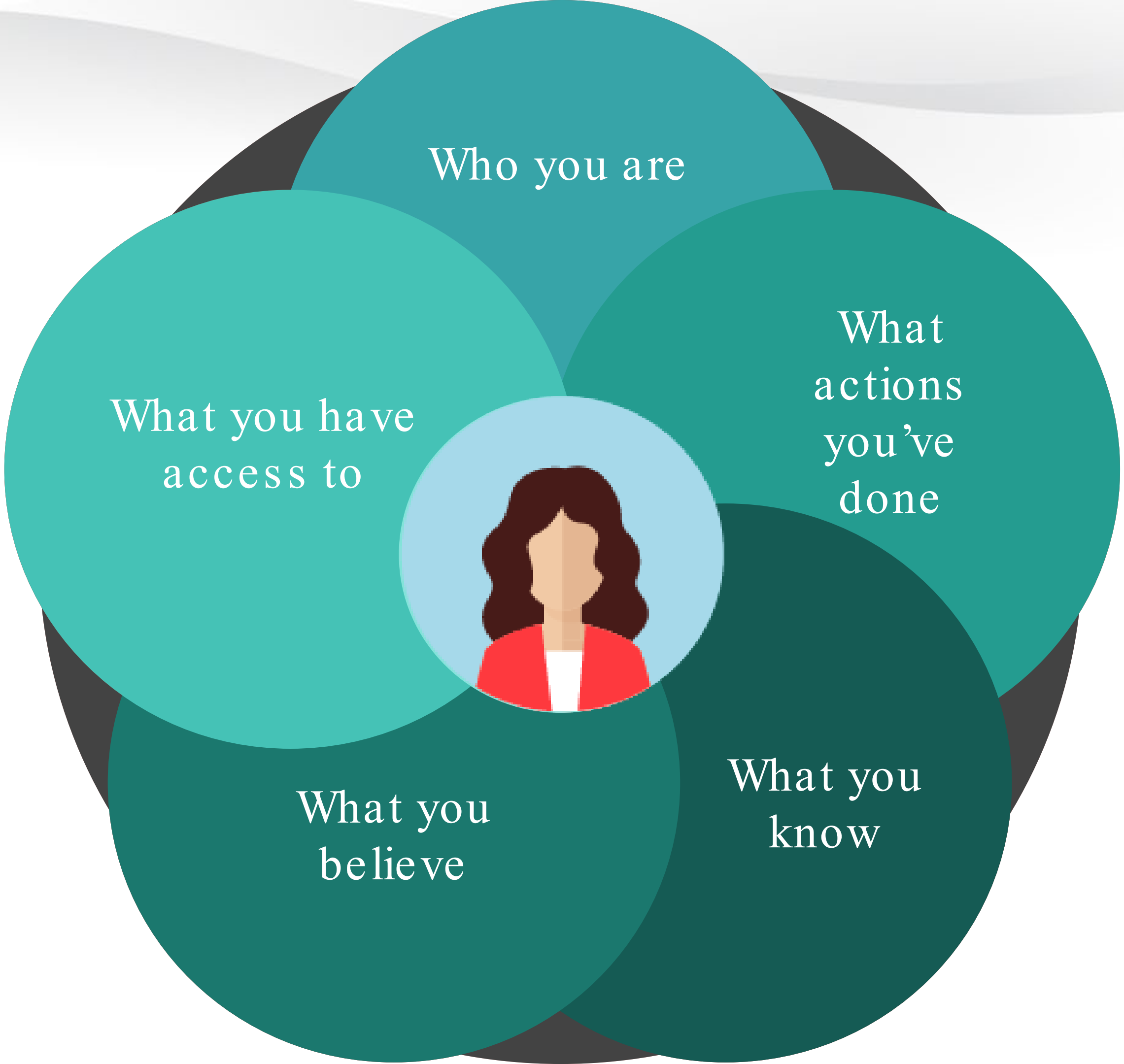
Only completed annual security training
Perfect mock phishing detection
Has production access



10+ hrs of of security training
Numerous malware incidents
Limited access to critical systems

New hire
No known trainings completed
No behavior baseline

360 Degree Security View



Who you are

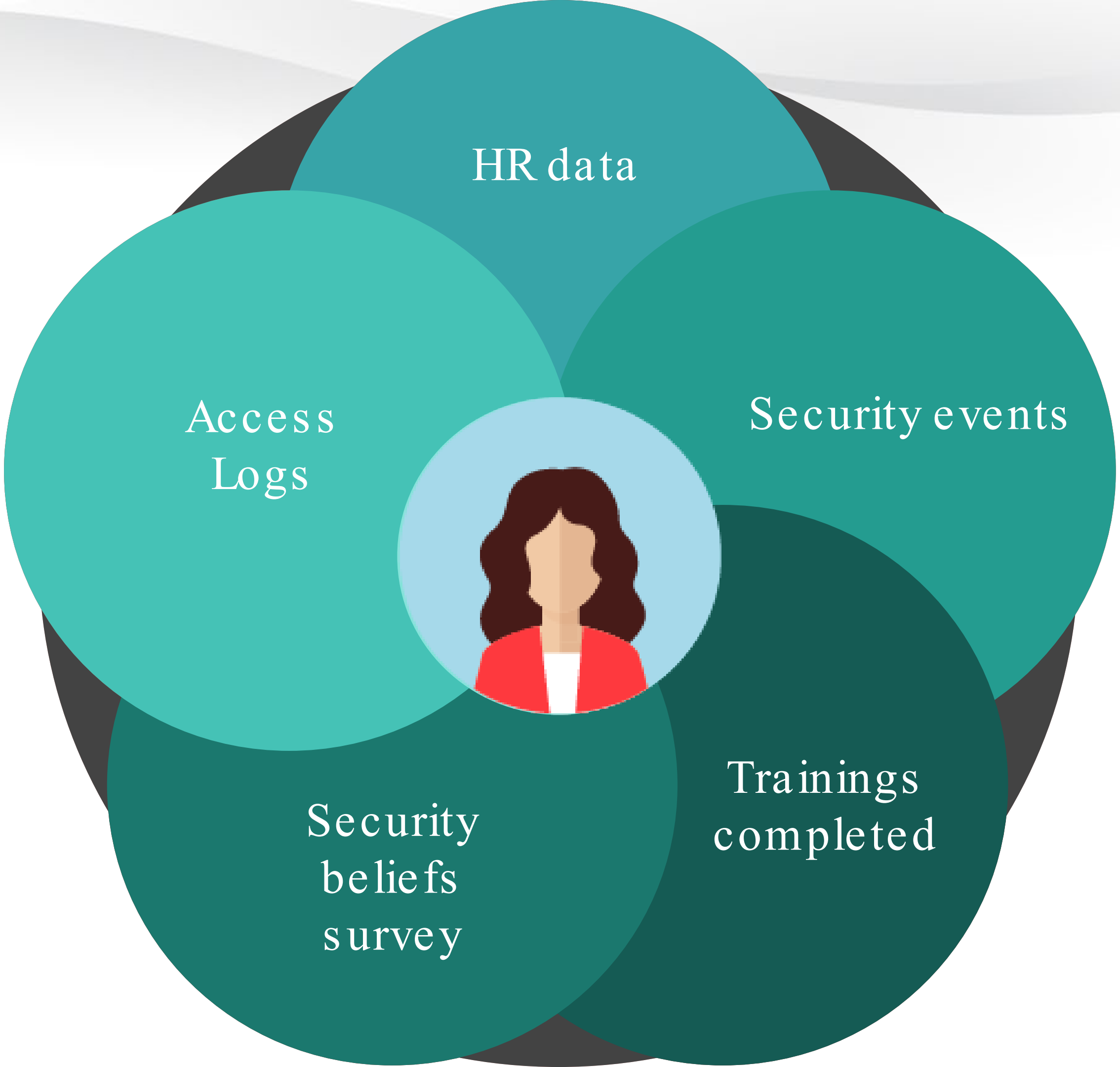
What actions you've done

What you know

What you believe

What you have access to

360 Degree Security View



How can we measure it?

HR Data

- Department
- Tenure
- Geography
- Seniority in company

Access > Role

What are your most critical systems?

- Access to production
- Ability to check in code
- Wire transfer
- Access to company sensitive information

Who has access to those systems?

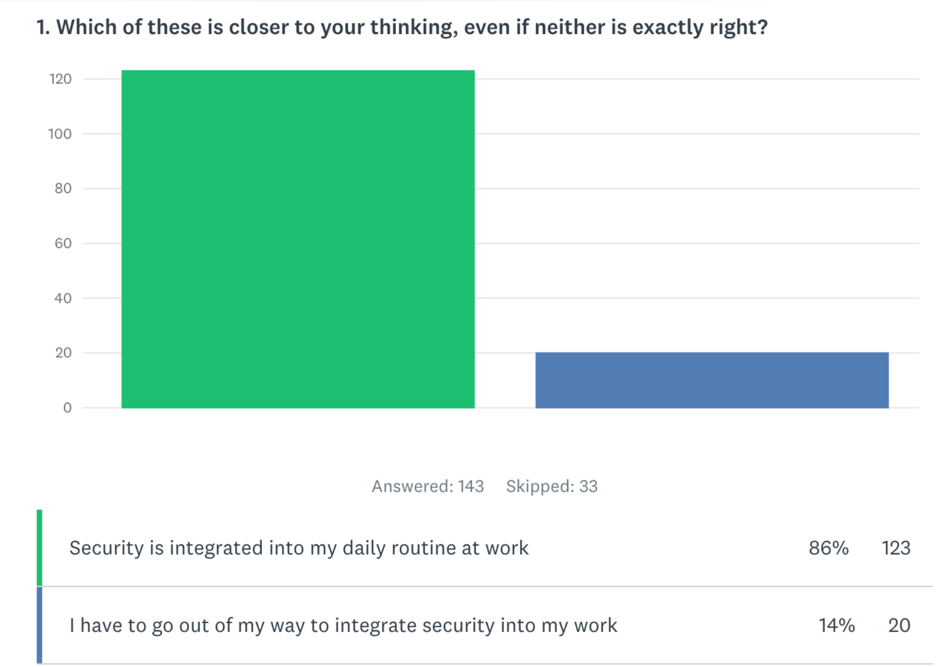
Measuring mindset- Security FORCE Survey

How do employees view security and the security team?

Do they feel empowered to take action for security issues?

Do employees feel the leadership team prioritizes security?

Survey resources:
https://www.surveymonkey.com/curiosity/building-a-security-culture-starts-with-measuring/



1. Which of these is closer to your thinking, even if neither is exactly right?

Answered: 143   Skipped: 33

Security is integrated into my daily routine at work	86%	123
I have to go out of my way to integrate security into my work	14%	20

Knowing Isn't Enough

WE UNDERSTAND WHAT GOOD PASSWORD BEHAVIOR SHOULD LOOK LIKE

59% know a secure password is important

91% understand the risk of reusing passwords

YET WE CONTINUE TO EXHIBIT POOR PASSWORD HABITS

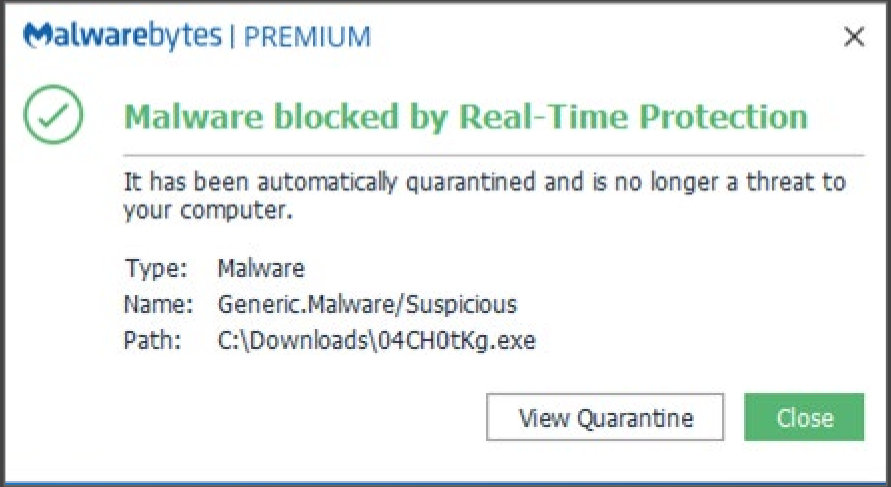
41% choose a password that is easy to remember

61% use the same or similar passwords

Lastpass 2017

The best predictor of future behavior is past behavior

Use the data you ***ALREADY HAVE***!

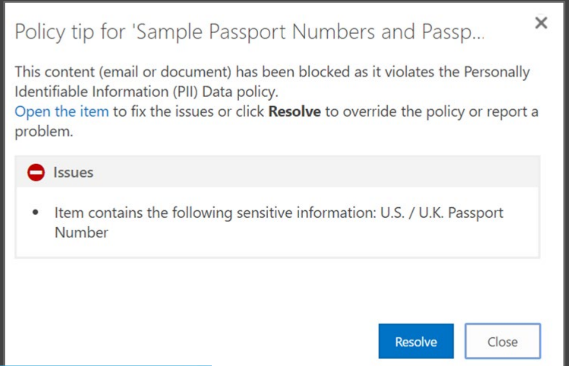


Malwarebytes | PREMIUM

Malware blocked by Real-Time Protection

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Generic.Malware/Suspicious
Path: C:\Downloads\04CH0tKg.exe

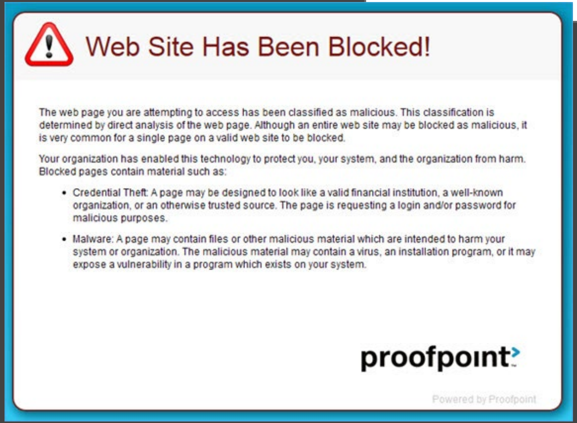


Policy tip for 'Sample Passport Numbers and Passp...

This content (email or document) has been blocked as it violates the Personally Identifiable Information (PII) Data policy.
Open the item to fix the issues or click **Resolve** to override the policy or report a problem.

Issues

- Item contains the following sensitive information: U.S. / U.K. Passport Number

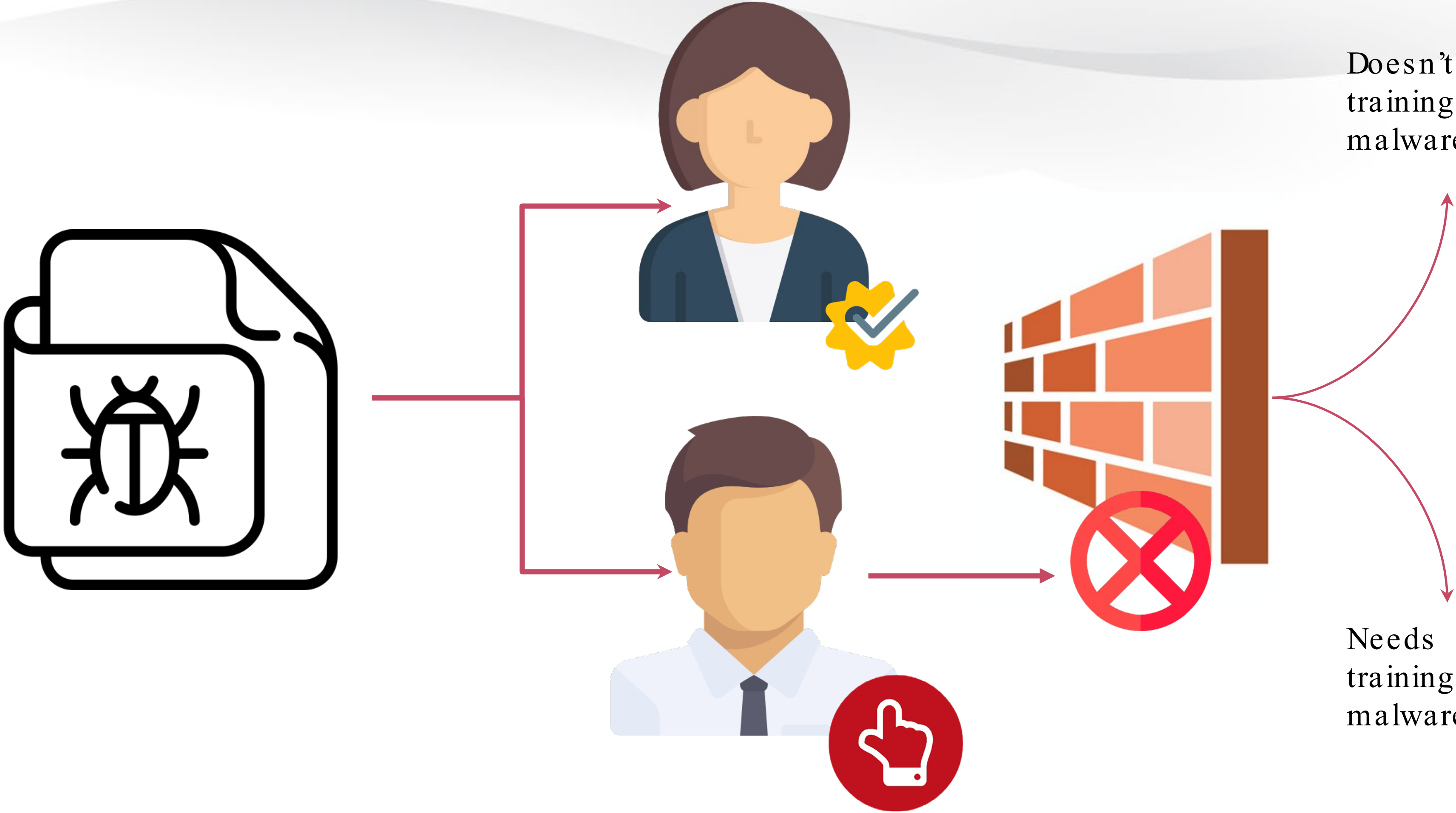


Web Site Has Been Blocked!

The web page you are attempting to access has been classified as malicious. This classification is determined by direct analysis of the web page. Although an entire web site may be blocked as malicious, it is very common for a single page on a valid web site to be blocked.

Your organization has enabled this technology to protect you, your system, and the organization from harm. Blocked pages contain material such as:

- Credential Theft: A page may be designed to look like a valid financial institution, a well-known organization, or an otherwise trusted source. The page is requesting a login and/or password for malicious purposes.
- Malware: A page may contain files or other malicious material which are intended to harm your system or organization. The malicious material may contain a virus, an installation program, or it may expose a vulnerability in a program which exists on your system.

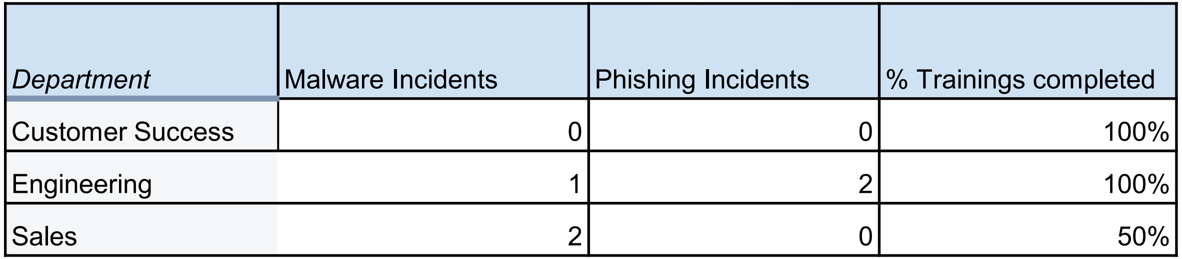


Doesn’t need training on malware

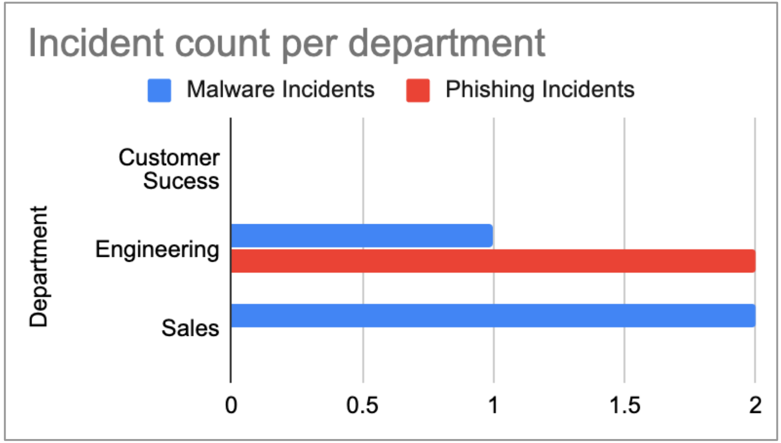
Needs training on malware

What do I do with this data once I have it?

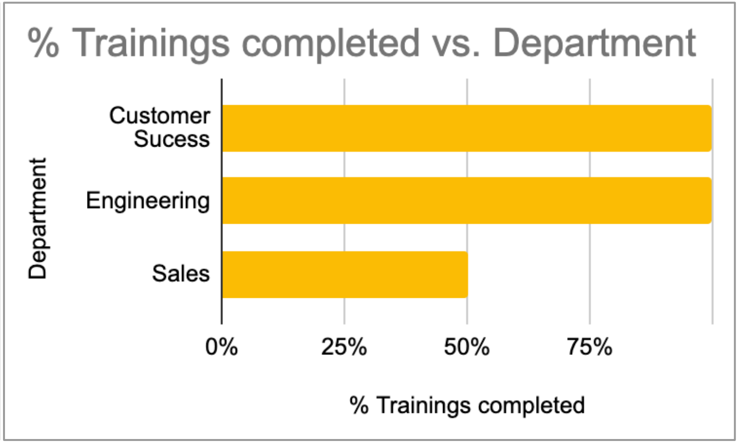
Level 1: Spreadsheets & Pivot Tables



Department	Malware Incidents	Phishing Incidents	% Trainings completed
Customer Success	0	0	100%
Engineering	1	2	100%
Sales	2	0	50%

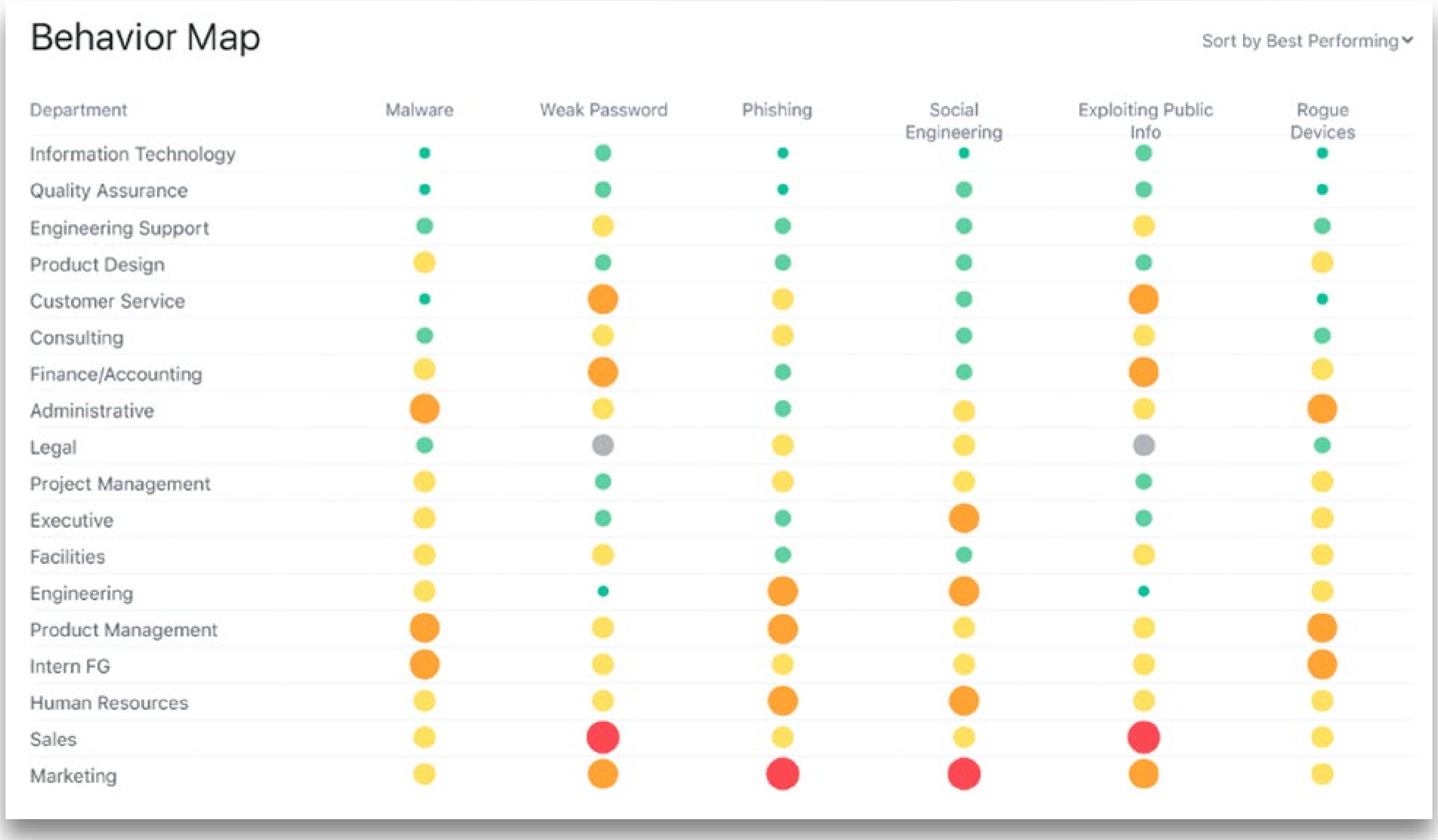


Incident count per department



% Trainings completed vs. Department

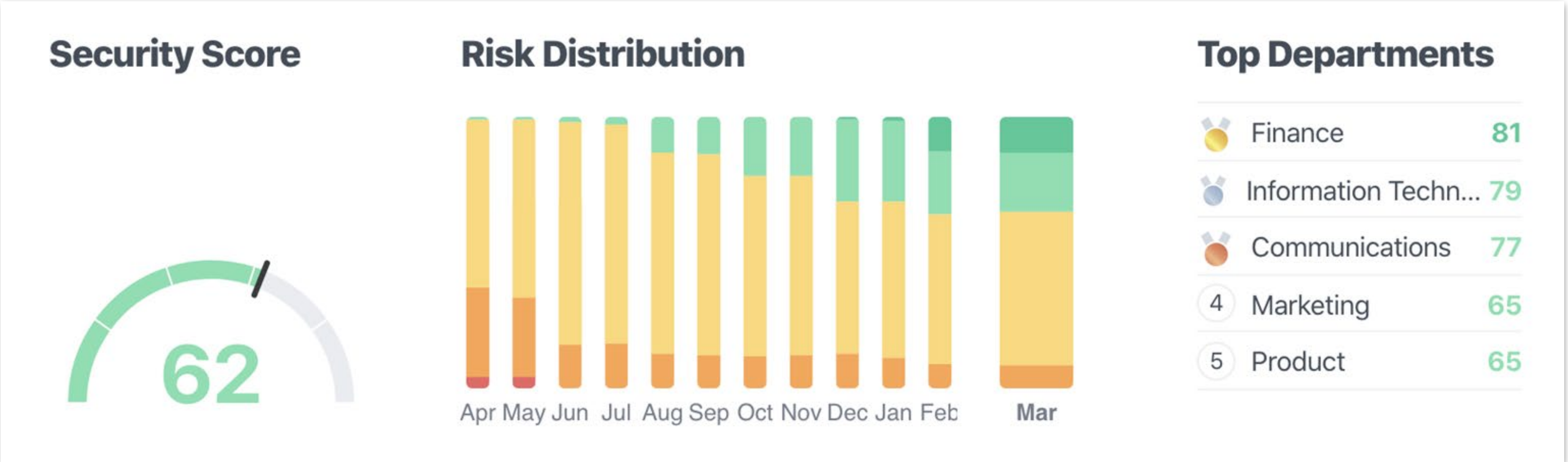
Level 2:Visualization



Behavior Map

Department	Malware	Weak Password	Phishing	Social Engineering	Exploiting Public Info	Rogue Devices
Information Technology	🟢	🟢	🟢	🟢	🟢	🟢
Quality Assurance	🟢	🟢	🟢	🟢	🟢	🟢
Engineering Support	🟢	🟡	🟢	🟢	🟡	🟢
Product Design	🟡	🟢	🟢	🟢	🟢	🟡
Customer Service	🟢	🟠	🟡	🟢	🟠	🟢
Consulting	🟢	🟡	🟡	🟢	🟡	🟢
Finance/Accounting	🟡	🟠	🟢	🟢	🟠	🟡
Administrative	🟠	🟡	🟢	🟡	🟡	🟠
Legal	🟢	⚪	🟡	🟡	⚪	🟢
Project Management	🟡	🟢	🟡	🟡	🟢	🟡
Executive	🟡	🟢	🟢	🟠	🟢	🟡
Facilities	🟡	🟡	🟢	🟢	🟡	🟡
Engineering	🟡	🟢	🟠	🟠	🟢	🟡
Product Management	🟠	🟡	🟠	🟡	🟡	🟠
Intern FG	🟠	🟡	🟡	🟡	🟡	🟠
Human Resources	🟡	🟡	🟠	🟠	🟡	🟡
Sales	🟡	🔴	🟡	🟡	🔴	🟡
Marketing	🟡	🟠	🔴	🔴	🟠	🟡

Level 3:Historical Trends & Comparisons



Security Score

62

Risk Distribution

Top Departments

	Finance	81
	Information Techn...	79
	Communications	77
4	Marketing	65
5	Product	65

RSAConference2020

Q&A

10 Minutes

What are you currently measuring?

What would be some additional security actions you could measure?

What behaviors to focus on?

Sensitive Data Handling

Password Hygiene

Phishing Susceptibility

Increase Reporting

Physical Security

Malware Infection

2FA Adoption

USB Usage

Using the internet safely

Mobile Security

How could you prioritize the most important ones?

How To Prioritize Key Behaviors

1. What are your most frequent incidents?
2. What would be the most damaging to your company?
3. What are easy wins?
4. What's most visible?
5. What would have the greatest impact on your security posture?
6. What does your team already have metrics on?

Where might you source the data from?

Where to Source Security Behavior Change Metrics

Sensitive Data Handling	Proxies - Bluecoat, ZScaler, Websense DLP - Vontu
Password Hygiene	Password Managers - LastPass, Keypass Active Directory Hash analysis
Phishing Susceptibility	Mock phishing- Elevate, Cofense, Knowbe4 Email security - Proofpoint, Mimecast
Increase Reporting	Reporter buttons, security inbox
Physical Security	Badge readers, manual surveys

Malware Infection	Endpoint - SentinelOne, Carbon Black, Cylance, Symantec, Trend
2FA Adoption	Auth providers- Duo, Okta
USB Usage	Endpoint - SentinelOne, Carbon Black, Cylance, Symantec, Trend
Using the internet safely	Proxies - Bluecoat, ZScaler, Websense Endpoint - SentinelOne, Carbon Black, Cylance, Symantec, Trend
Mobile Security	Endpoint - Lookout, ESET, Trend, etc MDM Vendors - Airwatch, MobileIron, Good, etc

Workshop

15 minutes

Discuss & Complete The Handout

1. What are the top behaviors your want to measure?
2. How might you be able to measure those behaviors?
3. Who are you stakeholders for that data?

Optional
What are your most critical systems?
Who has access to those systems?

Sample Worksheet

Behavior	Data Source	Owner
Real Phishing	Email security system	IT
Sensitive Data handling	Data loss prevention system	Security Architect
Password manager adoption	Enterprise password manager	Enterprise security team
Access	Data Source	Owner
Product Environment	All employees with Root	Production Engineering
Wire transfer	Transfer privileges in company billing system	Finance

Next Steps

- Next week you should:
  - Refine your Behavior Data Worksheet
- In the first three months following this presentation you should:
  - Socialize with key stakeholders on priority
  - Contact data set owners
  - Start getting data sets in!
- Within six months you should:
  - Use input to architect your program direction
  - Start tracking impact of campaigns

RSAConference2020

Questions? Comments?

Let’s stay in touch

masha@elevatesecurity.com