ALLIANCE Media Group

Alliances

DigitalAlliances

continue collaboration

CISO Alliances – UK&I
5th October 2021

In Partnership with :

proofpoint.

Alliance - ‘A union formed for mutual benefit’

Digital Alliances

continue collaboration

ALLIANCE Media Group

DigitalAlliances
continue collaboration

CISO Alliances

'The growing menace from within – Why insider threat is the biggest risk that firms face'

United Kingdom & Ireland

Andrew Rose, Resident CISO - Proofpoint

Tuesday 5th of October 10:30am (GMT)
www.alliances.global
james@alliances.global

In partnership with proofpoint

Session Leader:
Andrew Rose - Resident CISO - EMEA - Proofpoint
Session Title: **Debate: The growing menace from within - Why insider threat is the biggest risk that firms face**

Session Synopsis

For many years, insider threat has been a topic that CISOs have acknowledged but taken little action to address. The infrequent events were generally low impact, and could usually be managed outside the public eye.

The accelerated digital transformation driven by the pandemic has complicated matters as firms have rushed toward remote working and cloud adoption to solve their challenges. Unfortunately these changes been equally advantageous to the attackers who can now compromise employees and access your corporate network under assumed identities.

The CISOs challenge now is how to differentiate between a well-meaning employee bending a policy to delight a client, and an external attacker using a compromised account for their own ends.

Join Andrew Rose, Proofpoint's Resident CISO, for this discussion regarding insider threat where we will consider

Why insider risk is fast becoming the primary attack path;
Tools and techniques CISOs use to and prioritise identify insider risks;
Pragmatic controls to reduce the likelihood and potential impact of insider risk.

DigitalAlliances
continue collaboration

Food For Thought/Topics Discussed

proofpoint.

The Growing Menace From Within - Why Insider Threat Is The Biggest Risk That Firms Face

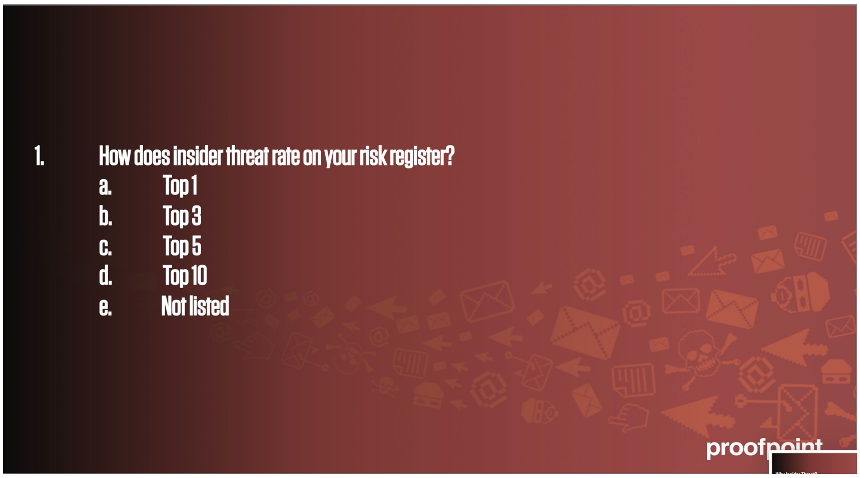
Andrew Rose, Resident CISO, Proofpoint

Why Insider Threat?

proofpoint.

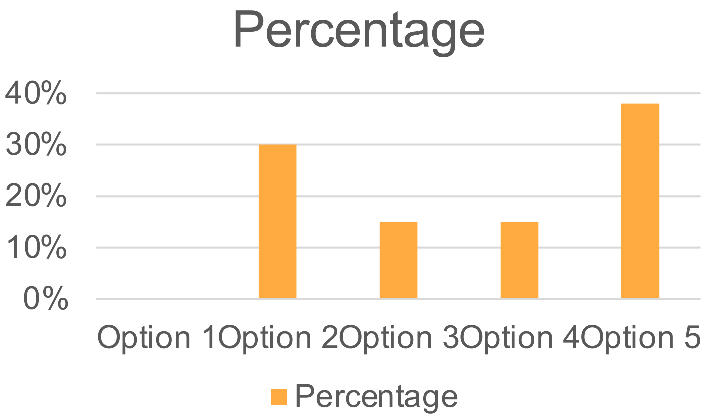
Digital Alliances
continue collaboration

Food For Thought/Topics Discussed

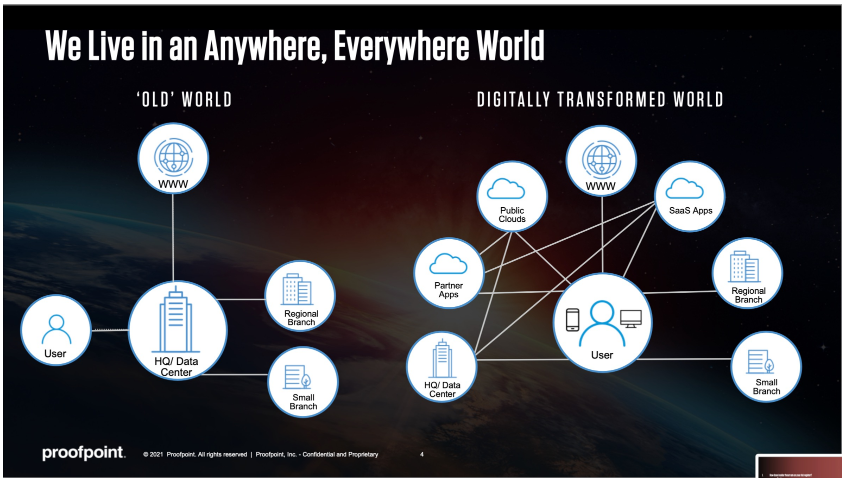


1. How does insider threat rate on your risk register?
   a. Top 1
   b. Top 3
   c. Top 5
   d. Top 10
   e. Not listed

In Session Poll Results



Food For Thought/Topics Discussed

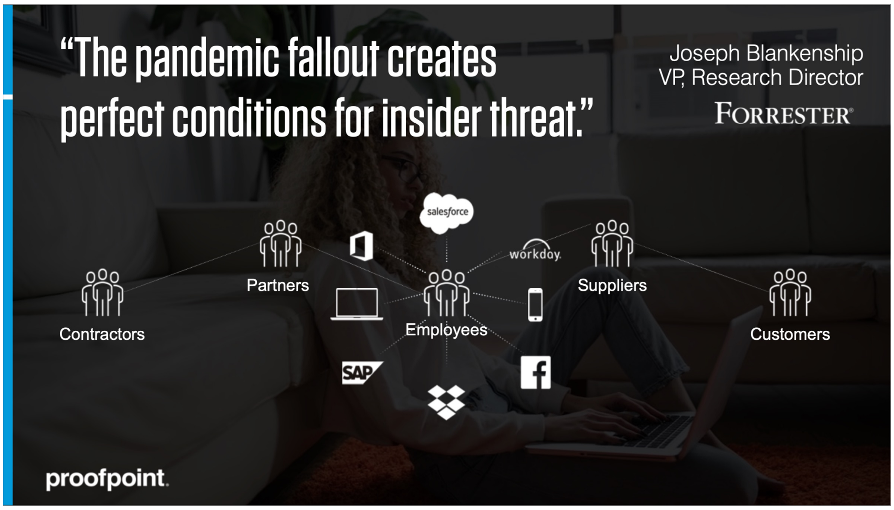


We Live in an Anywhere, Everywhere World

proofpoint. © 2021 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary 4

- I think we all recognize that digital transformation has really changed our organizations.
- Organizations used to be a data center, infrastructure, physicality sort of centric model, where everything would come back to the HQ or through this sort of major data center. we all recognize that we're now in a very different environments, digital transformation has changed the way we architect our organizations. And we now adopt software as a service cloud technology. We use a lot of third parties and partners. And what that does is that changes the way that the model looks and what it does.
- It places the user at the center of this new architecture. So what happens at this point really is that identity becomes the new perimeter rather than the physicality. And unfortunately, that means that users then become the primary attack surface because that's the way to access any of the assets within the enterprise.

Food For Thought/Topics Discussed

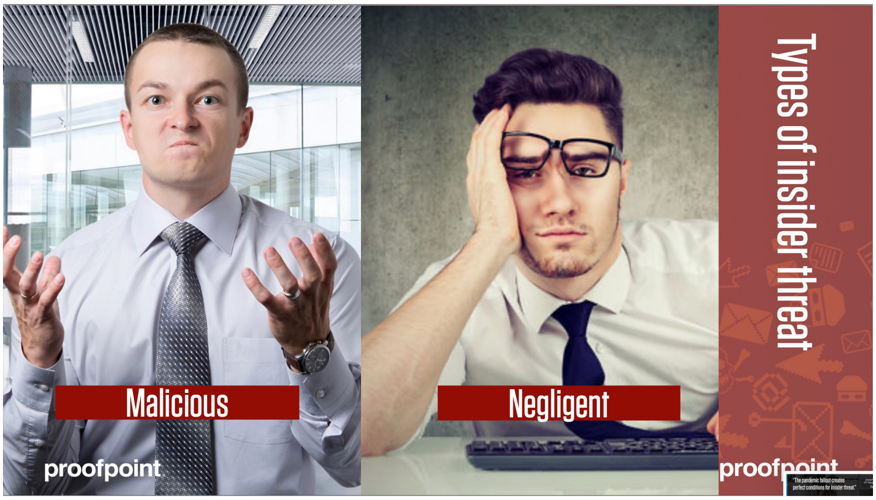


"The pandemic fallout creates perfect conditions for insider threat."

Joseph Blankenship
VP, Research Director
FORRESTER

- Having the user at the center of the enterprise increases the threats, there's more to it than that from the COVID perspective. There's new endpoints, both physical and virtual, whether people are using their own PCs or using Citrix end points to connect into the enterprise new endpoints, alongside that you get new applications.
- And you've got the challenge of monitoring the activity and all the data within those systems, whether they're known or unknown, to protect all of you.
- We're also meeting or hiring staff without ever meeting them. Face-to-face. So I've met very few of my proof point colleagues, because I've started since COVID lockdown happened and I'm sure lots of organizations do the same.
- And then finally, you've got the staff dissatisfaction, the financial repercussions of COVID means that jobs have been cut. Bonuses are being cut. Promotions are being passed over. All of those things are going to increase threats in terms of the insider threats.

Food For Thought/Topics Discussed



Types of insider threat

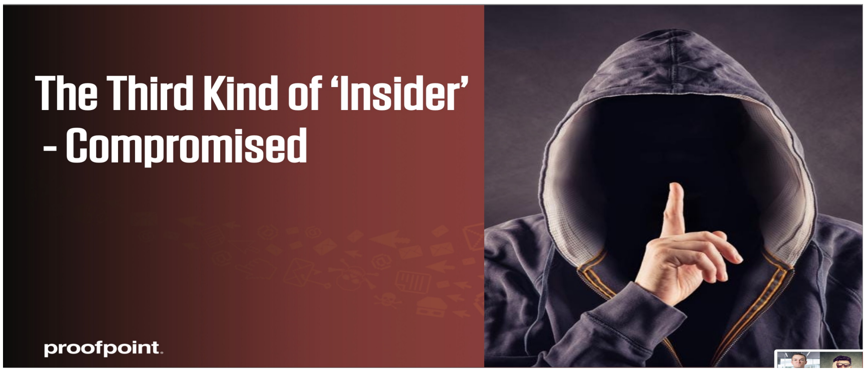
Malicious

Negligent

proofpoint

"The pandemic fallout creates perfect conditions for insider threat."

- Negligent users can make horrific mistakes.
- You can get people who will take in information for their own benefits.



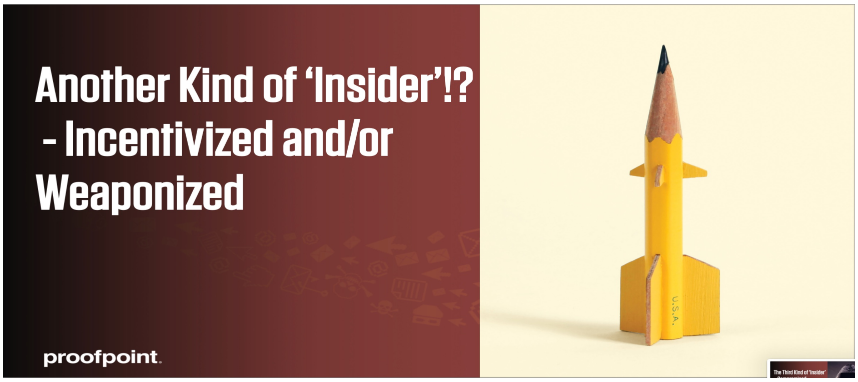
The Third Kind of 'Insider' - Compromised

proofpoint

- If an account is stolen and abused attackers can use that to deliver content or steal intellectual property, or do all those insider threats.
- They look like an insider because it is using legitimate account.
- This is much more challenging than those other two accounts, but these are the two insider types because, a negligent user is making a mistake or pushing boundaries or breaking policy. And they're doing it probably to achieve a work-related goal. They're not trying to do it to damage your organization, as a compromised user is absolutely trying to damage your organization. A malicious person is possibly detectable.

DigitalAlliances
continue collaboration

Food For Thought/Topics Discussed

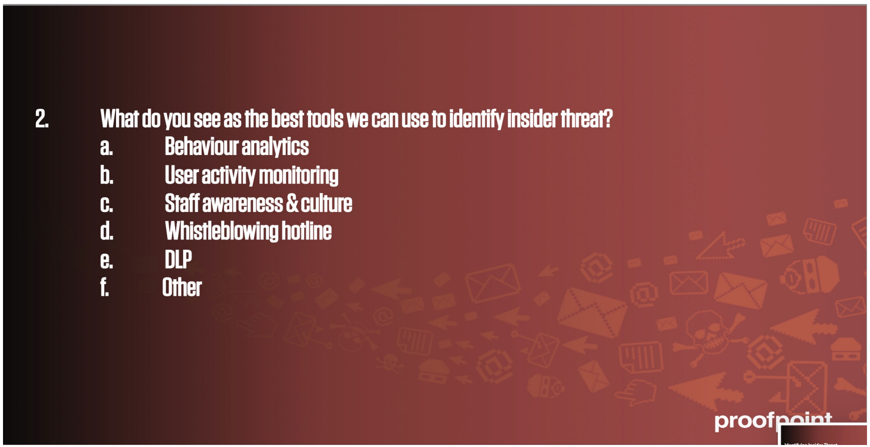


Another Kind of 'Insider'!? - Incentivized and/or Weaponized

proofpoint.

- The fourth type is an extension to malicious, and that is weaponized users or incentivized users. It's a way of taking those disgruntle or borderline malicious staff and pushing them over the line
- And there's two good examples of this. We've seen recently. One is Tesla where an employee was offered a million dollars to go and plug in a USB stick into a window server.
- One was something called demon ware, where people were being encouraged to trigger ransomware and they would get a cut of the profits.
- There's this weaponization, where attackers are trying to incentivize users to do the bad thing as well, which is also coming into the insider threats.
- Microsoft themselves said this last year that half a percent of office 365 accounts are compromised every month. And that's an astoundingly high number.
- And I expect that everybody here uses multi-factor authentication and that's a really good control against this, but it's no silver bullets. The attackers are focusing their efforts on bypassing multifactor authentication and certainly have used office 365.
- When you look at the malicious content and emails about 60% of malicious content in emails is all about credential theft.

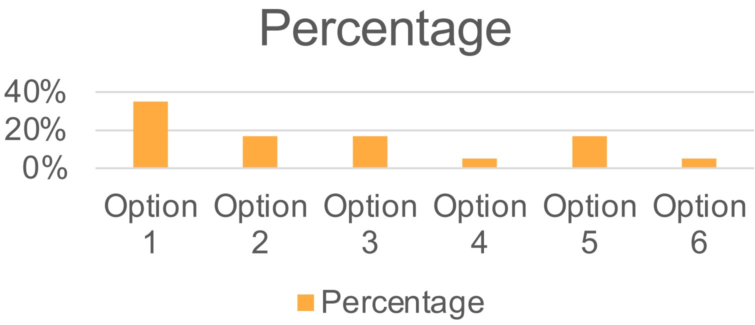
Food For Thought/Topics Discussed



2. What do you see as the best tools we can use to identify insider threat?
   a. Behaviour analytics
   b. User activity monitoring
   c. Staff awareness & culture
   d. Whistleblowing hotline
   e. DLP
   f. Other

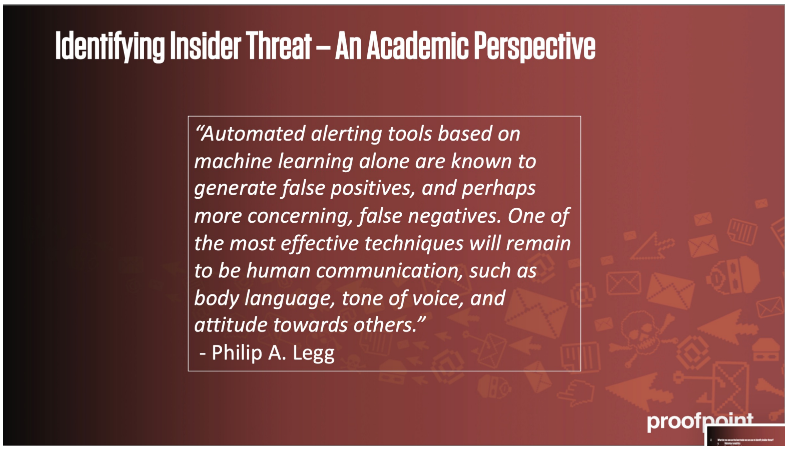
proofpoint

In Session Poll Results



- The key thing that comes out academia reports is that one of the most effective techniques is that human communication aspect.
- The results of the poll show otherwise, and Andrew agrees.

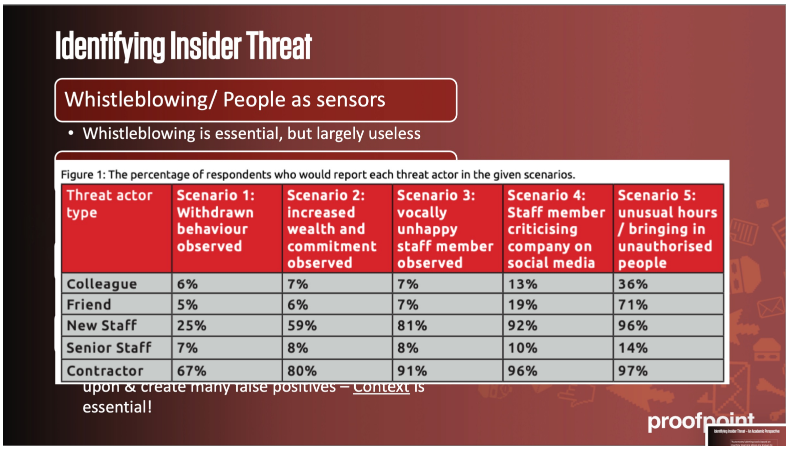
Food For Thought/Topics Discussed



Identifying Insider Threat – An Academic Perspective

> *"Automated alerting tools based on machine learning alone are known to generate false positives, and perhaps more concerning, false negatives. One of the most effective techniques will remain to be human communication, such as body language, tone of voice, and attitude towards others."*
> - Philip A. Legg

proofpoint



Identifying Insider Threat

Whistleblowing/ People as sensors

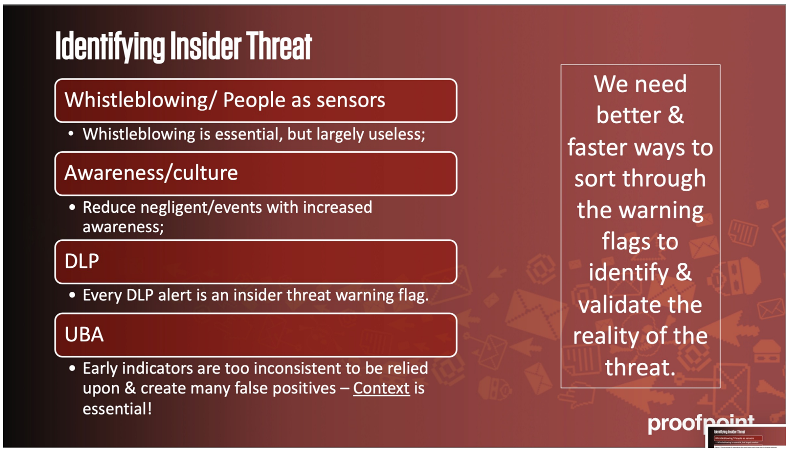
- Whistleblowing is essential, but largely useless

Figure 1: The percentage of respondents who would report each threat actor in the given scenarios.

Threat actor type	Scenario 1: Withdrawn behaviour observed	Scenario 2: increased wealth and commitment observed	Scenario 3: vocally unhappy staff member observed	Scenario 4: Staff member criticising company on social media	Scenario 5: unusual hours / bringing in unauthorised people
Colleague	6%	7%	7%	13%	36%
Friend	5%	6%	7%	19%	71%
New Staff	25%	59%	81%	92%	96%
Senior Staff	7%	8%	8%	10%	14%
Contractor	67%	80%	91%	96%	97%

upon & create many false positives – Context is essential!

proofpoint



Identifying Insider Threat

Whistleblowing/ People as sensors

- Whistleblowing is essential, but largely useless;

Awareness/culture

- Reduce negligent/events with increased awareness;

DLP

- Every DLP alert is an insider threat warning flag.

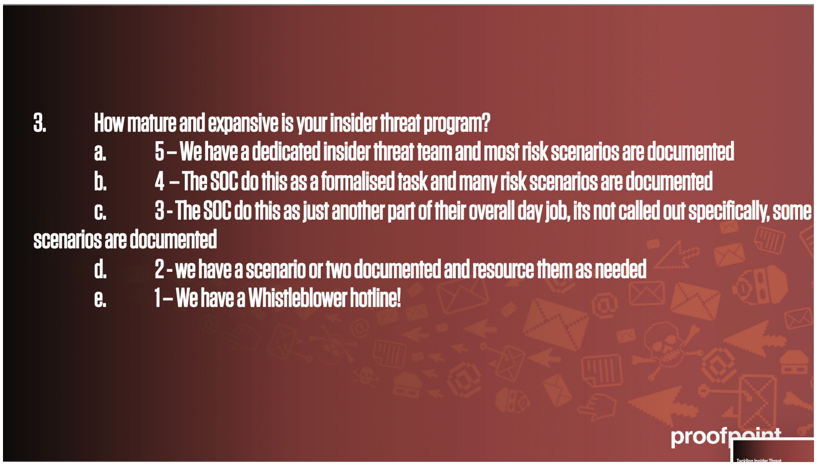
UBA

- Early indicators are too inconsistent to be relied upon & create many false positives – Context is essential!

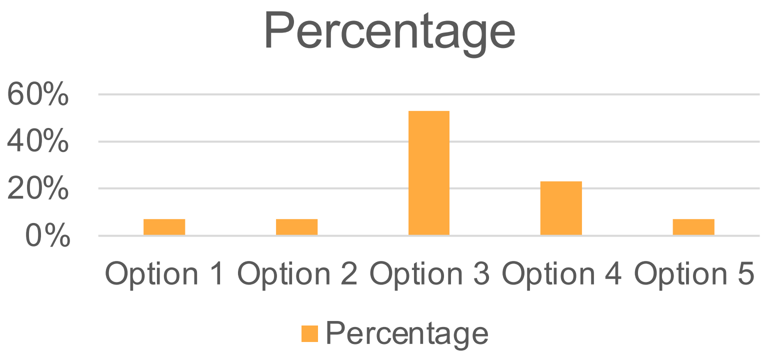
We need better & faster ways to sort through the warning flags to identify & validate the reality of the threat.

proofpoint

Food For Thought/Topics Discussed



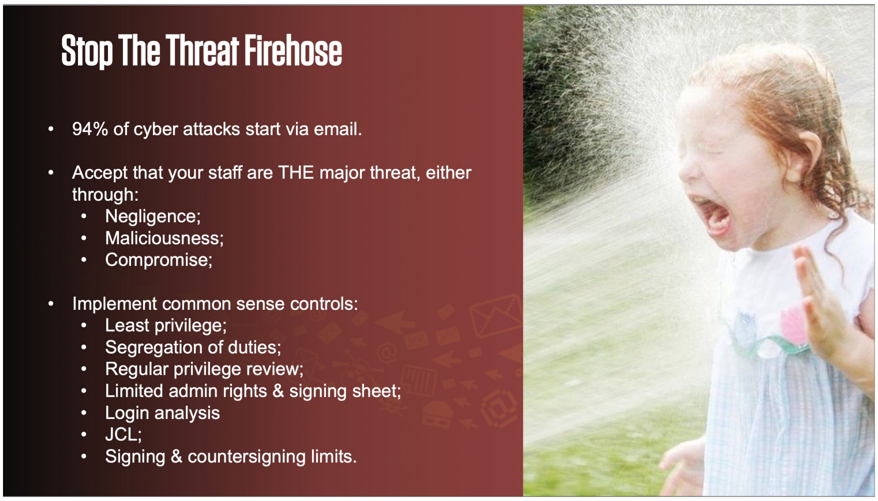
3. How mature and expansive is your insider threat program?
   a. 5 – We have a dedicated insider threat team and most risk scenarios are documented
   b. 4 – The SOC do this as a formalised task and many risk scenarios are documented
   c. 3 - The SOC do this as just another part of their overall day job, its not called out specifically, some scenarios are documented
   d. 2 - we have a scenario or two documented and resource them as needed
   e. 1 – We have a Whistleblower hotline!



DigitalAlliances

continue collaboration

Food For Thought/Topics Discussed



Stop The Threat Firehose

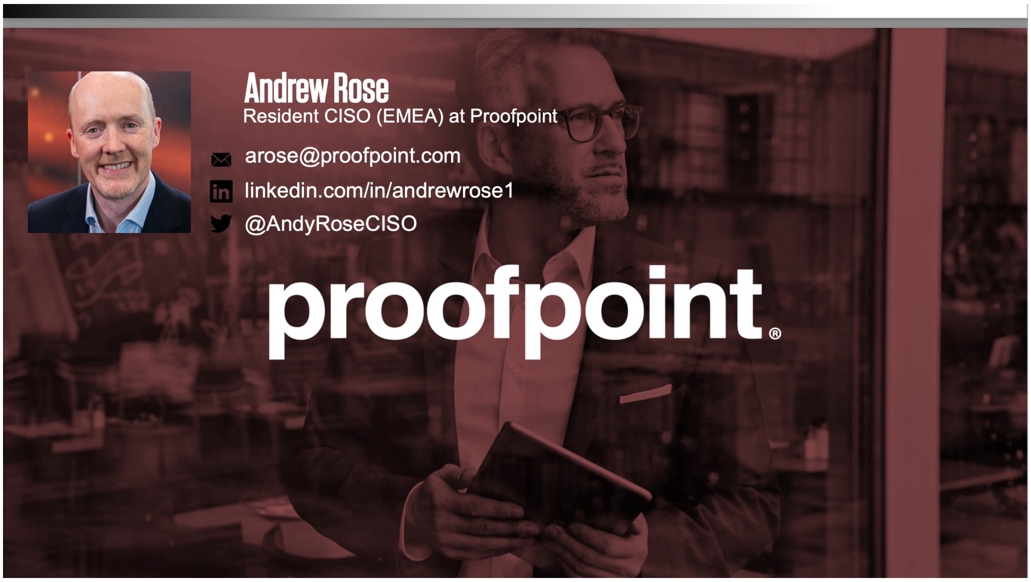
- 94% of cyber attacks start via email.
- Accept that your staff are THE major threat, either through:
  - Negligence;
  - Maliciousness;
  - Compromise;
- Implement common sense controls:
  - Least privilege;
  - Segregation of duties;
  - Regular privilege review;
  - Limited admin rights & signing sheet;
  - Login analysis
  - JCL;
  - Signing & countersigning limits.

- Privileged segregation of duties, limited admin rights, regular privilege review login analysis checked, joiners, changes and leavers.
- Organisations go through the process of assembling cross functional teams from different departments, figuring out what the couple of risks scenarios are, is it intellectual property theft from labs, whatever it happens to be. They will come up with a couple of scenarios which are biggest in terms of potential business impact.
- And then they work those through and say, okay, well what would the alarms could we get, if this was happening, what errors would we see? What alerts would would be created and how do we then validate those alerts, the steps we would go through, who would we fire and who would we speak to?
- What data would we look at to correlate and figure out whether this is real or whether this is just somebody doing the best they can for the organization, because, you know, is this somebody just sending work home for the weekend so they can delight the client on Monday? Or is this the start of somebody stealing intellectual property? Or is this, you know, the start of the real malicious ransomware attack, they all have very different responses, but actually at the initial stage, they may all look very similar.

DigitalAlliances

continue collaboration

Food For Thought/Topics Discussed



Andrew Rose
Resident CISO (EMEA) at Proofpoint

✉ arose@proofpoint.com
in linkedin.com/in/andrewrose1
@AndyRoseCISO

proofpoint®

DigitalAlliances
continue collaboration