NTP attacks

In 2014, hackers started using NTP reflection attacks.

This created unprecedented levels of bandwidth consumption. Where attackers would have been previously focusing on application layer attacks to cause your servers to crash, now they were able to cripple the country where your servers were hosted to ensure you went down.

Before the attacks happened, the attackers tested the potency of their capability on random targets. Then they planned the attack and fulfilled it with all their might, almost "breaking the Internet".

One of the key takeaways, is that they tested the attack first, for a few seconds before the real one. By detecting such network anomalies, important assumptions can be made, such as "why am I suddenly receiving tons of NTP responses to my Web Server"?

The fifth domain of warfare

It has become a realization for those who have already been breached

...and for those who haven't detected it yet.

While you advance and evolve, in order to defend against the emerging threats

... the threats will also continue to counter-evolve.

Think like the attacker.

This talk is about..

[illegible]

Understanding Cyber Resiliency

[illegible]

Challenges ?

[illegible]

secure → monitor → detect / predict → prevent → respond → recover

- Secure as fast as possible.
- Fix problems on-the-fly, immediately and effectively.
- Fix the problems faster than your systems can currently detect these problems
- The only commonality in some cases, is anomaly on the network.
- Detect unknown threats.
- Contextual awareness.

Towards a Cyber Resilience strategy

[illegible]

Contract

NEWS

A "Cyber Resilience strategy" has become the next logical step for defending against the unavoidable evolution of threats.

Defence mechanisms need to constantly counter-evolve against the counter-evolution of emerging threats, in order to be able to detect, prevent, respond, recover and further evolve.

This type of constant need for scalability and adaptation becomes even more challenging and demanding when it meets complex systems, which are also high-value targets.

Jump on the cyber-evolution train..

- Move beyond outdated solutions and **ask** the right questions
- Up to what level **risk** should be considered acceptable?
- Demonstrate **Due Diligence** to avoid claims of negligence.
- Consider **Cyber Insurance** coverage.
- Have a dynamic & equally evolving resilience plan capable of responding to evolving threats which also allows you to **stay within budget**.

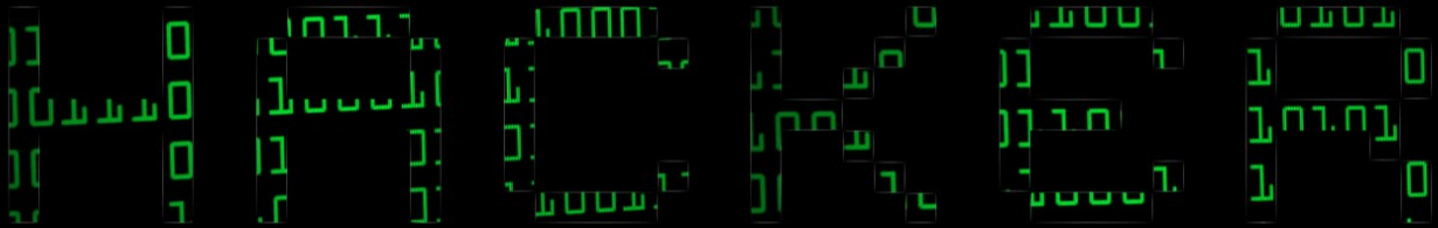
BALCCON2K17
U CNT CTRL ME

Moving Towards Cyber Resilience

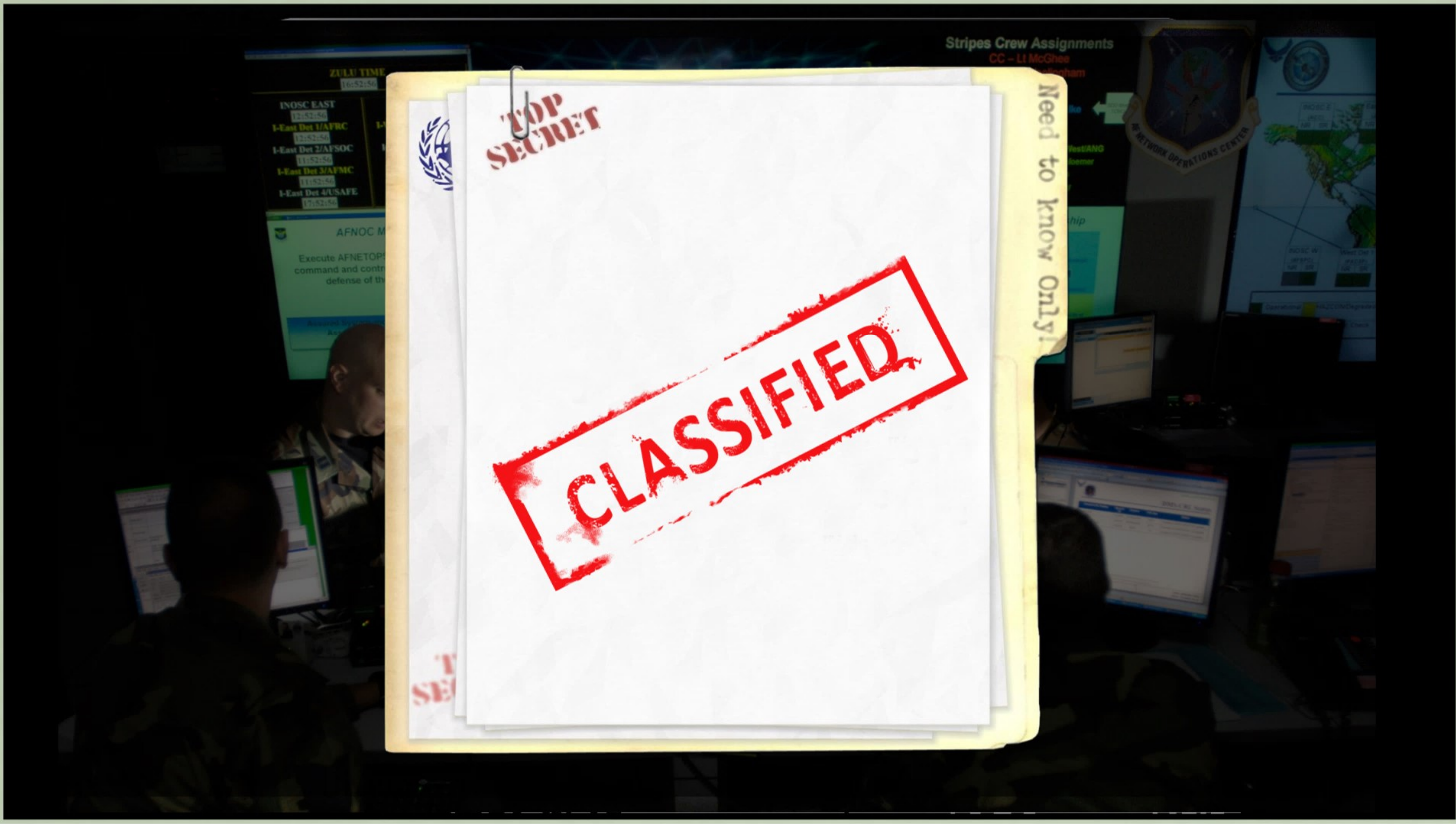
Dr. Grigorios Fragkos

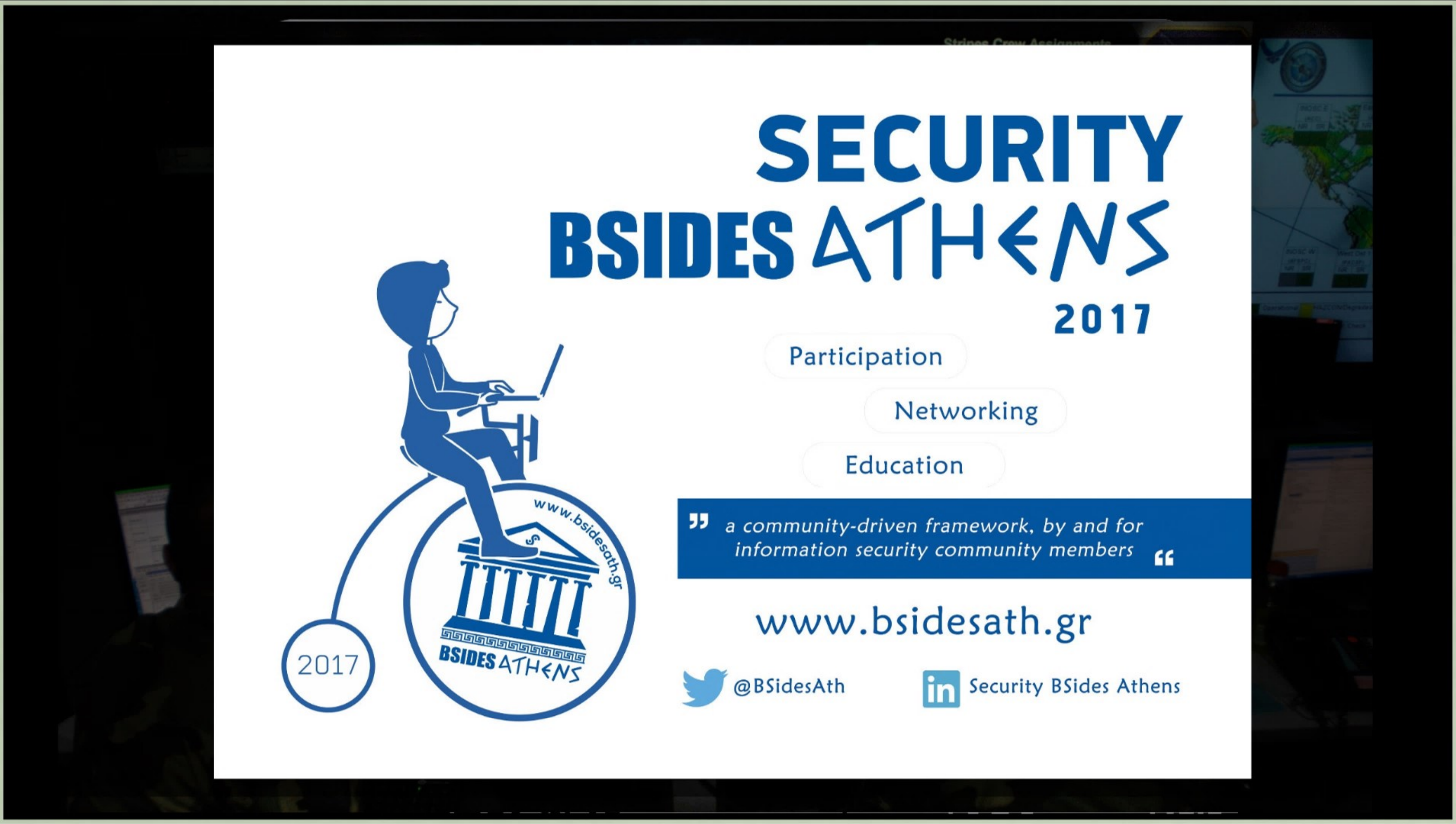
@drgfragkos

about me



HACKER


TOP SECRET
CLASSIFIED
Need to know Only!
Stripes Crew Assignments
ZULU TIME
INOSC EAST
AFNOC



SECURITY BSIDES ATHENS

2017

Participation

Networking

Education

> ” a community-driven framework, by and for information security community members “

www.bsidesath.gr

@BSidesAth

Security BSides Athens

BSides Amsterdam

www.bsidesams.nl

@BSidesAMS

Stripes Crew Assignments

@BSidesAMS

Stripes Crew Assignments
sidesAMS
ingenico
@drgfragkos
IPP350
F1
F2
F3
F4
MENU
CANCEL
CLEAR
ENTER

This talk is about..

- Familiarise the audience with the term Cyber Resilience

- On how a holistic approach to information security problems today, will allow to better ourselves in most aspects of cybersecurity when it comes to safeguarding our companies, organisations, and businesses, worldwide.

- How Cyber Resilience will change the way the board thinks, as it can be measurable and effective, without spending more (sometimes even less)

- Bridge the gap between the "Ethical Hacker" and the Board of Directors

@drgfragkos

Understanding Cyber Resiliency..

- It is a term that goes beyond a Business Continuity Plan (BCP) and Disaster Recovery (DR).

- It is a broad holistic approach to address CyberSecurity challenges, that includes readiness, response, and recovery, at a broad ecosystem.

- Cyber Resilience demands the collaboration of the board, technologists, the involvement of third-parties, cybersecurity experts, while responsibilities, regulations and compliance issues have been clarified, and tested.

@drgfragkos

Challenges ?

- Not traditional networks..
- Attacks against heterogeneous systems..
- Conventional methods of detection.. vs.
- Counter-evolving threats..
- Dynamically assigned resources..
- Fast adaptation & scalability..
- Holistic approach to the cyber security posture

@drgfragkos

A strategy for Cyber Resiliency..

- The board understands the need for Cyber Resiliency,

- Identify major risks (cyber resiliency risk assessment), the current exposure to threats, vulnerabilities, mission critical systems, high-value targets.

- Communicate across all departments and build an up-to-date cyber risk profile of the company. Do not oversee the third-party vendors (S/W, H/W), suppliers, contractors, and any other dependencies.

- Prioritize cyber resiliency activities, based on staff expertise, availability, budget, the bigger picture and by looking at least six months into the future.

@drgfragkos

The fifth domain of warfare

- Has become a realization for those who have already been breached,

- ..and for those who haven’t detected it yet.

- While you advance and evolve, in order to defend against the emerging threats,

- ..the threats will also continue to counter-evolve.

- Think like the attacker.

- **Think outside-of-the-box**

@drgfragkos

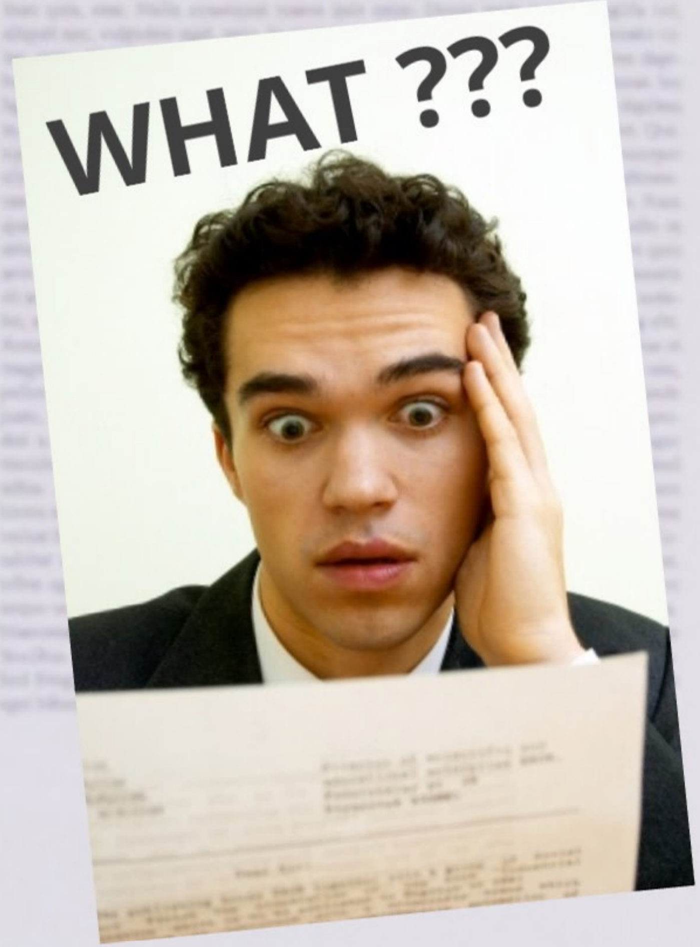
NTP attacks

In 2014, hackers started using NTP reflection attacks.

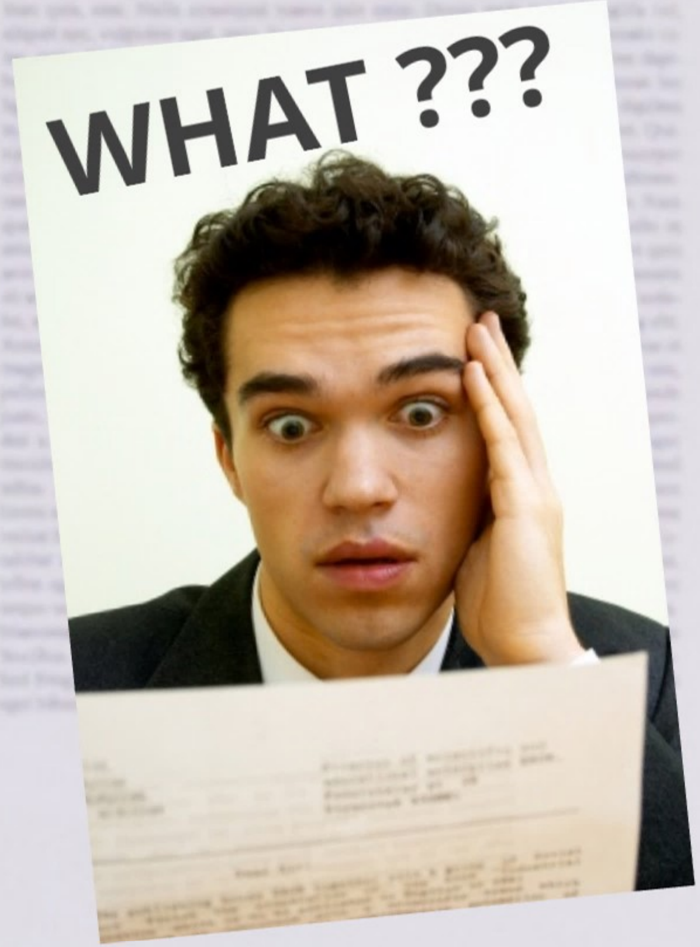
This created unprecedented levels of bandwidth consumption. Where attackers would have been previously focusing on application-layer attacks to cause your servers to crash, now they were able to cripple the country where your servers were hosted to ensure you went down.

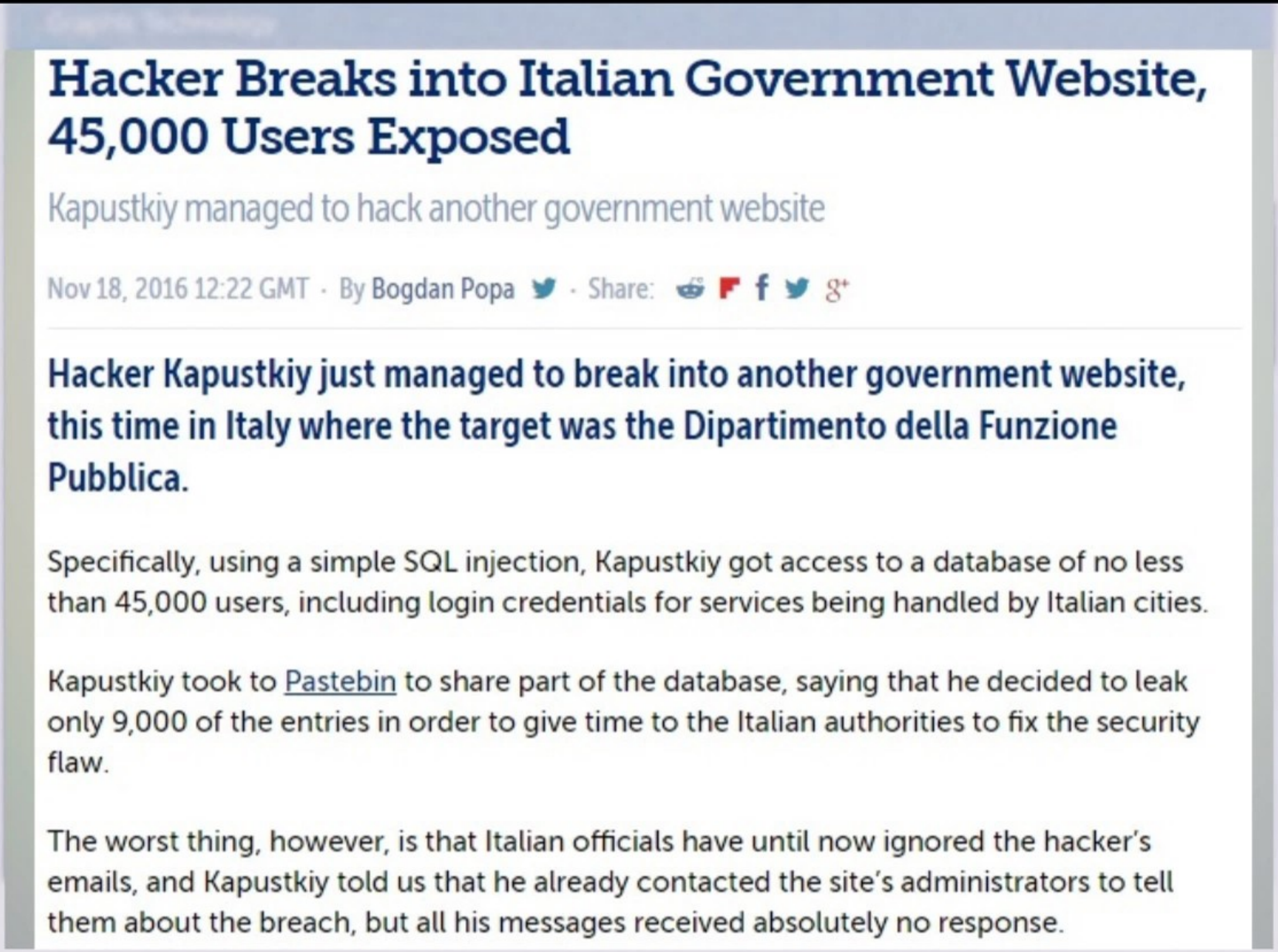
Before the attacks happened, the attackers tested the potency of their capability on random targets. Then they planned the attack and fulfilled it with all their might, almost "breaking the Internet".

One of the key takeaways, is that they tested the attack first, for a few seconds before the real one. By detecting such network anomalies, important assumptions can be made, such as “why am I suddenly receiving tons of NTP responses to my Web Server”?


WHAT ???

NETWORK
www
SOCiAL
@
Internet
www
@





Hacker Breaks into Italian Government Website, 45,000 Users Exposed

Kapustkiy managed to hack another government website

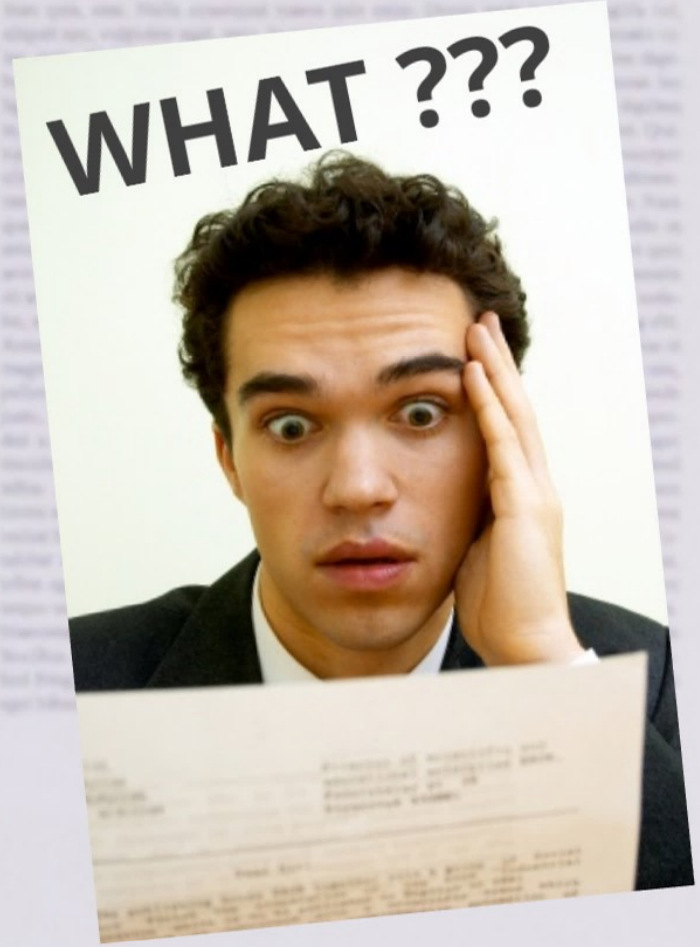
Nov 18, 2016 12:22 GMT · By Bogdan Popa · Share:

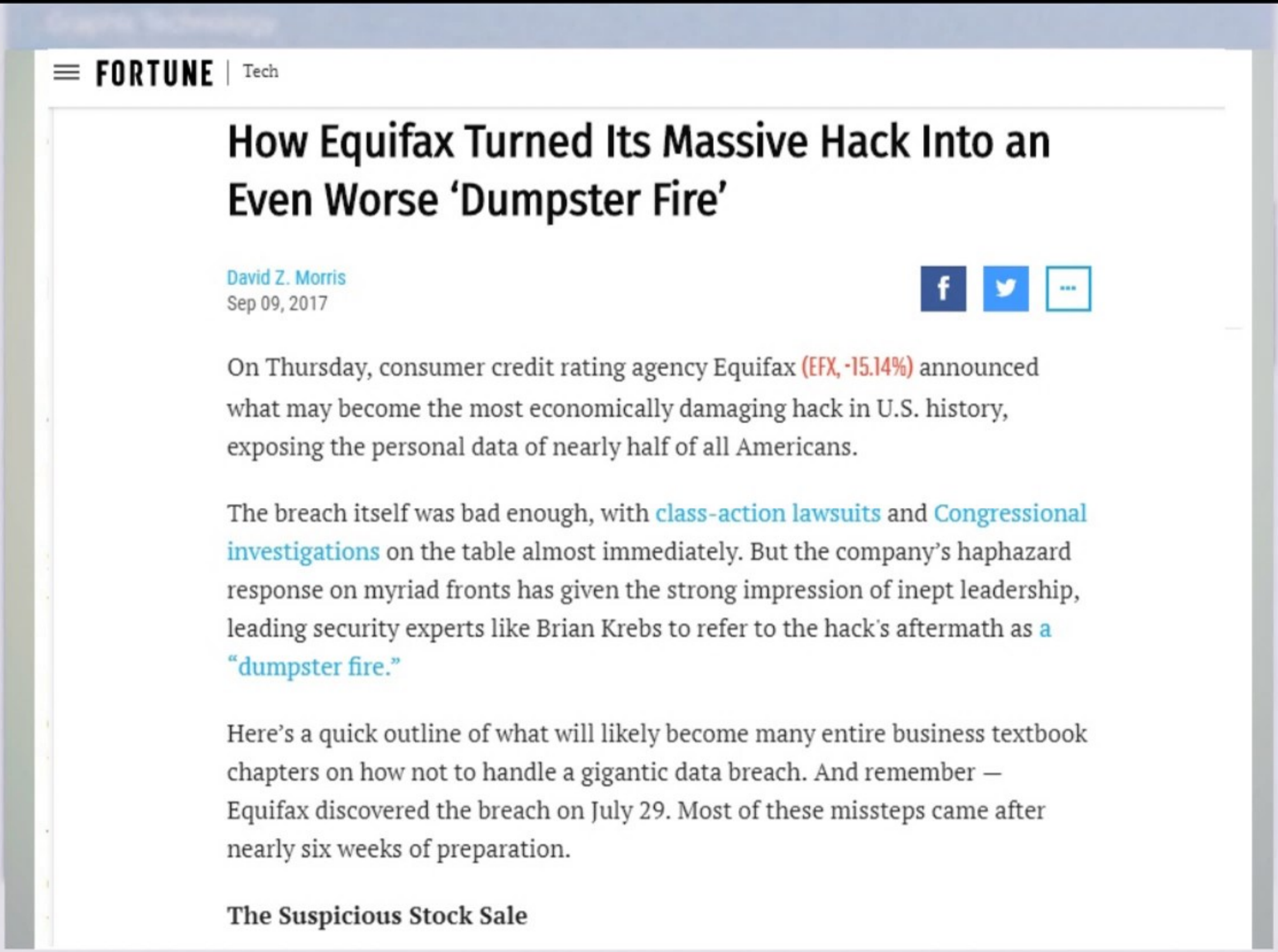
Hacker Kapustkiy just managed to break into another government website, this time in Italy where the target was the Dipartimento della Funzione Pubblica.

Specifically, using a simple SQL injection, Kapustkiy got access to a database of no less than 45,000 users, including login credentials for services being handled by Italian cities.

Kapustkiy took to Pastebin to share part of the database, saying that he decided to leak only 9,000 of the entries in order to give time to the Italian authorities to fix the security flaw.

The worst thing, however, is that Italian officials have until now ignored the hacker's emails, and Kapustkiy told us that he already contacted the site's administrators to tell them about the breach, but all his messages received absolutely no response.





How Equifax Turned Its Massive Hack Into an Even Worse 'Dumpster Fire'

David Z. Morris
Sep 09, 2017

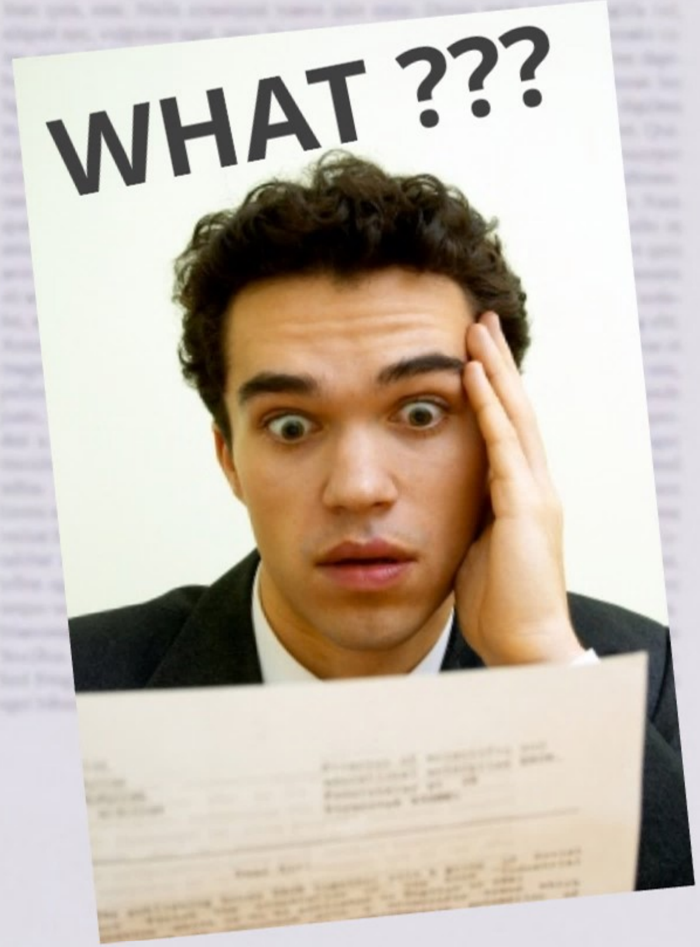
On Thursday, consumer credit rating agency Equifax (EFX, -15.14%) announced what may become the most economically damaging hack in U.S. history, exposing the personal data of nearly half of all Americans.

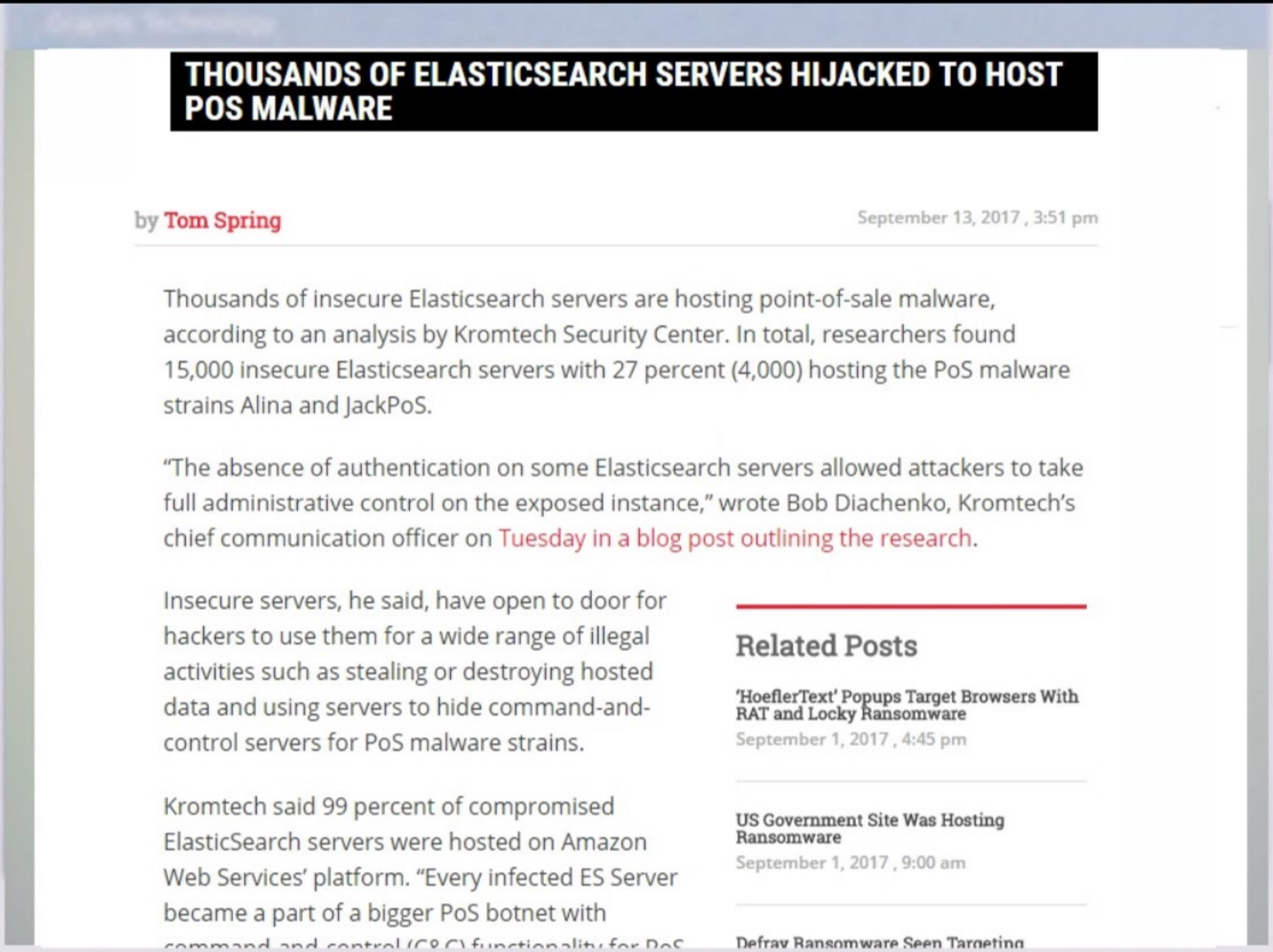
The breach itself was bad enough, with class-action lawsuits and Congressional investigations on the table almost immediately. But the company's haphazard response on myriad fronts has given the strong impression of inept leadership, leading security experts like Brian Krebs to refer to the hack's aftermath as a "dumpster fire."

Here's a quick outline of what will likely become many entire business textbook chapters on how not to handle a gigantic data breach. And remember — Equifax discovered the breach on July 29. Most of these missteps came after nearly six weeks of preparation.

The Suspicious Stock Sale

@drgfragkos





THOUSANDS OF ELASTICSEARCH SERVERS HIJACKED TO HOST POS MALWARE

by Tom Spring

September 13, 2017 , 3:51 pm

Thousands of insecure Elasticsearch servers are hosting point-of-sale malware, according to an analysis by Kromtech Security Center. In total, researchers found 15,000 insecure Elasticsearch servers with 27 percent (4,000) hosting the PoS malware strains Alina and JackPoS.

"The absence of authentication on some Elasticsearch servers allowed attackers to take full administrative control on the exposed instance," wrote Bob Diachenko, Kromtech's chief communication officer on Tuesday in a blog post outlining the research.

Insecure servers, he said, have open to door for hackers to use them for a wide range of illegal activities such as stealing or destroying hosted data and using servers to hide command-and-control servers for PoS malware strains.

Kromtech said 99 percent of compromised ElasticSearch servers were hosted on Amazon Web Services' platform. "Every infected ES Server became a part of a bigger PoS botnet with command-and-control (C&C) functionality for PoS

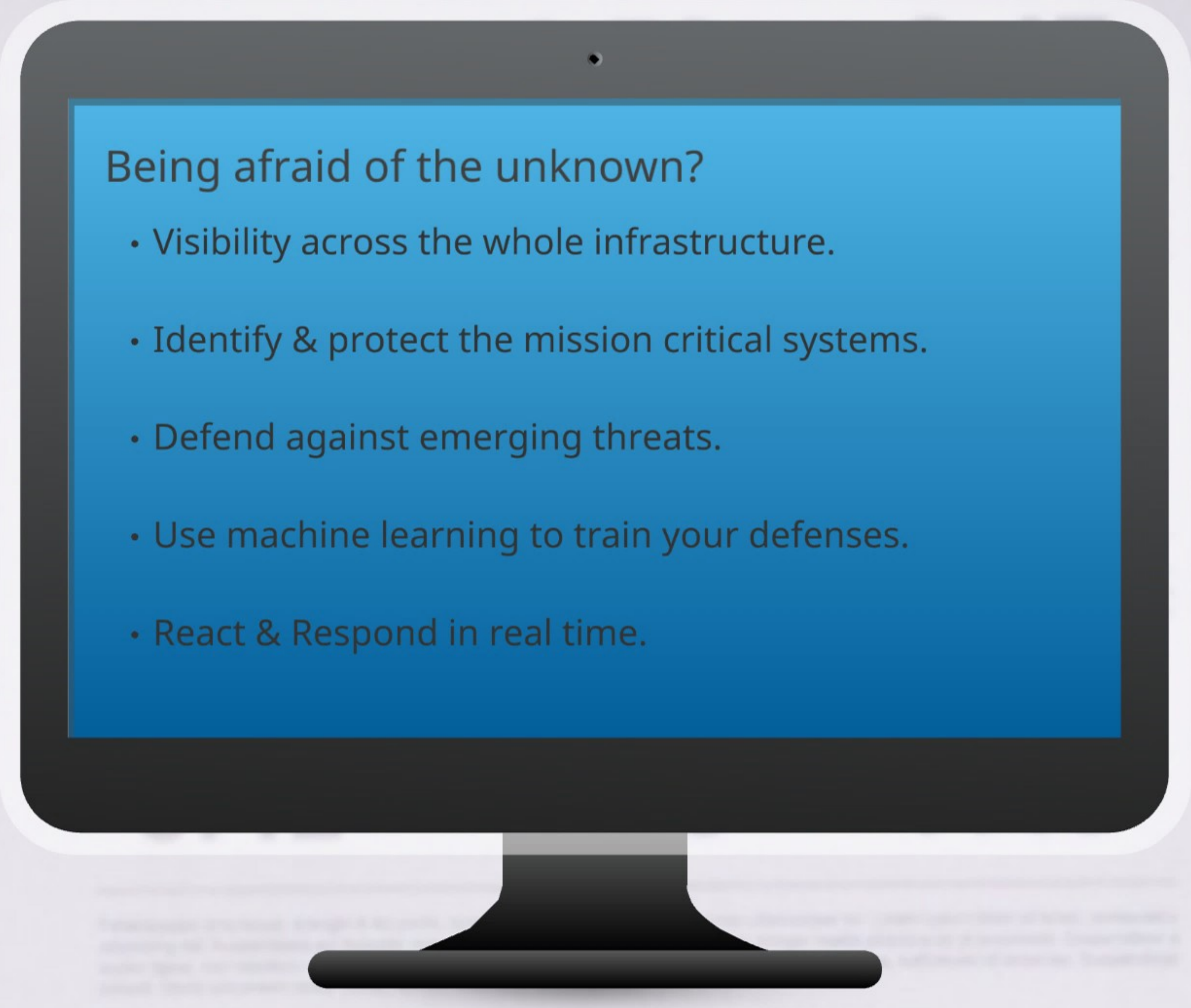
Related Posts

'HoeflerText' Popups Target Browsers With RAT and Locky Ransomware
September 1, 2017 , 4:45 pm

US Government Site Was Hosting Ransomware
September 1, 2017 , 9:00 am

Defray Ransomware Seen Targeting

@drgfragkos



Being afraid of the unknown?

- Visibility across the whole infrastructure.
- Identify & protect the mission critical systems.
- Defend against emerging threats.
- Use machine learning to train your defenses.
- React & Respond in real time.

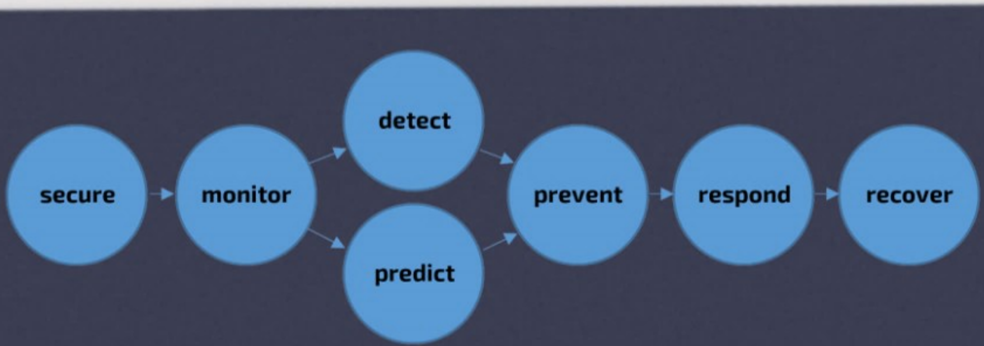
@drgfragkos

Being afraid of the unknown?

- Visibility across the whole infrastructure.
- Identify & protect the mission critical systems.
- Defend against emerging threats.
- Use machine learning to train your defenses.
- Detect & Respond in real time.

Cyber Criminals are opportunists!

@drgfragkos



- Secure as fast as possible.
- Fix problems on-the-fly, immediately and effectively.
- Fix the problems faster than your systems can currently detect these problems.
- The only commonality in some cases, is anomaly on the network.
- Detect unknown threats.
- Contextual awareness.

@drgfragkos

Towards a Cyber Resiliance strategy..

- Ensure a holistic security posture (internal/external).
  80% of attacks can be prevented with a few simple proactive measures and a preventive culture (Center of Internet Security).

- Be meticulous by using services that provide solutions to your specific problems and needs. (highly adjustable solutions)

- Focus on scalable, rapidly deployable solutions, forward-looking (e.g. GDPR), flexible (e.g. include IoT, Scada, etc.), adaptive (e.g. fraud)

- Ensure visibility across the whole infrastructure, while knowing yourself* and which are your mission critical assets.

@drgfragkos

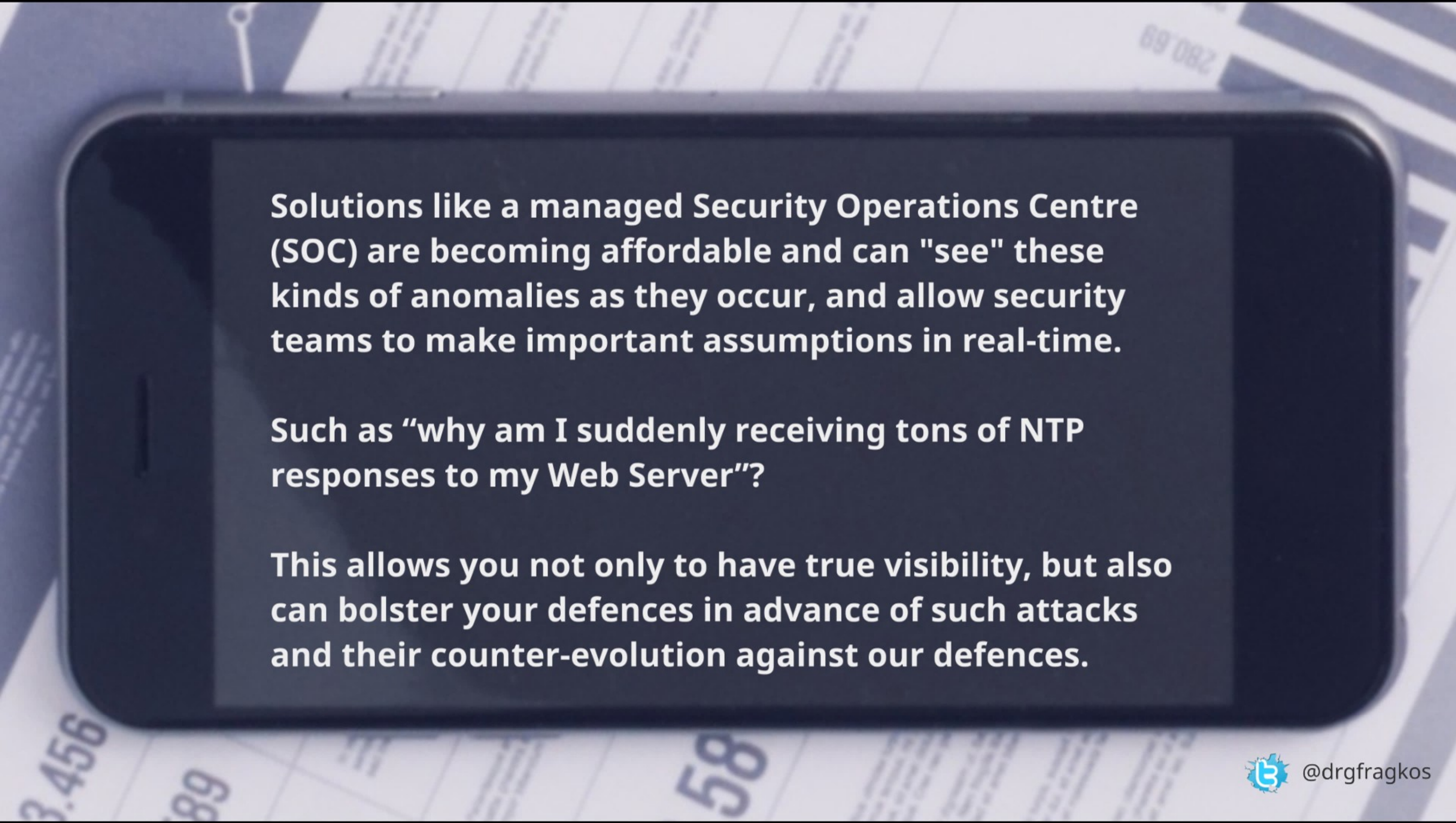
Towards a Cyber Resiliance strategy..

- Treat the need for Cyber Security in a systemic way identifying gaps & risks across the whole organisation/business.

- Stop introducing cracks & weak points by treating securing in an ad-hoc manner. It gets more expensive by having that approach.

- Devise a plan for threats and their effect to the business such as lost revenue, reputational harm, stock price (manipulation), etc..

- Key Performance Indicators (KPI). A business metric used to evaluate factors crucial to the success of an organization.

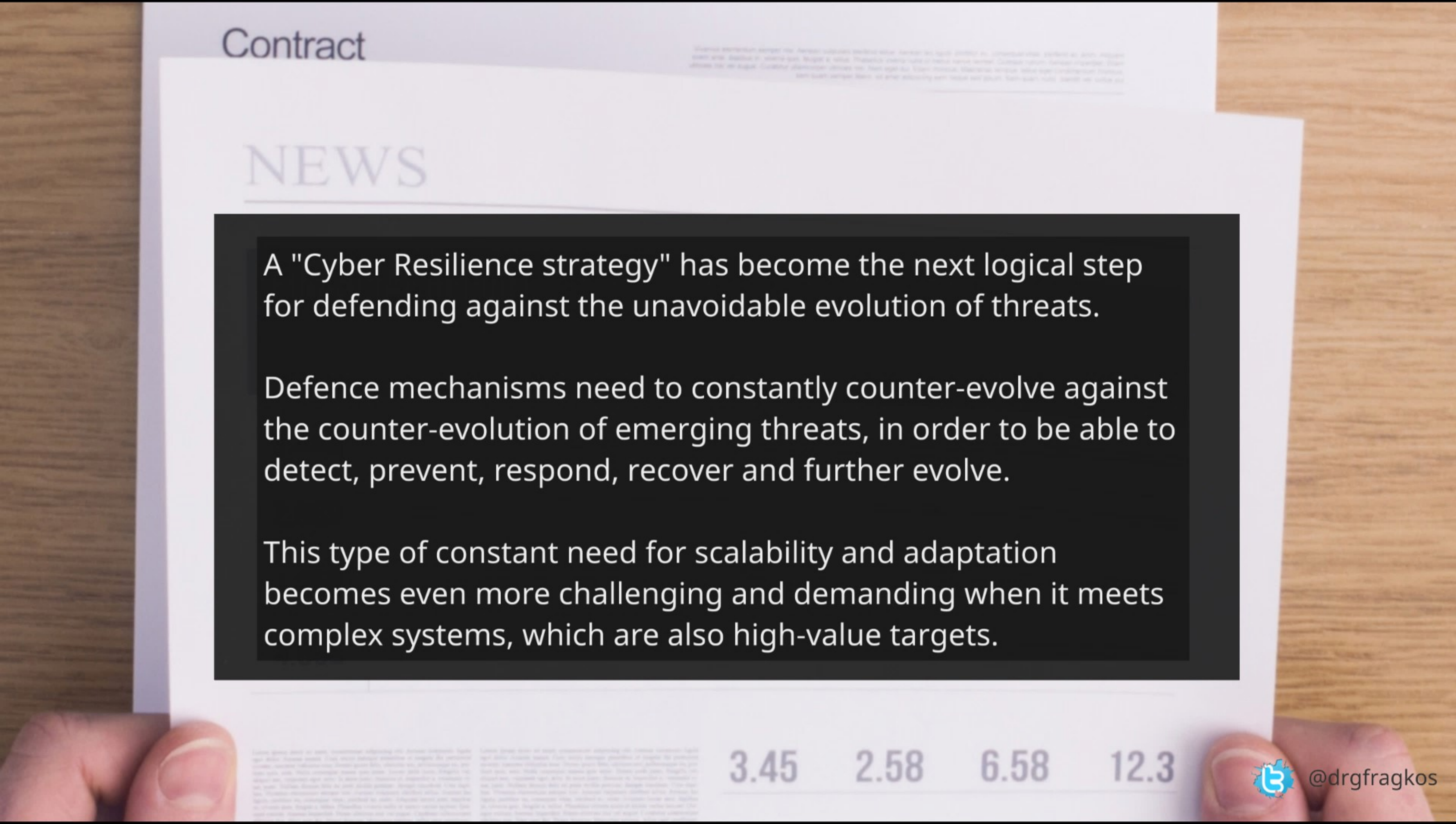


Solutions like a managed Security Operations Centre (SOC) are becoming affordable and can "see" these kinds of anomalies as they occur, and allow security teams to make important assumptions in real-time.

Such as “why am I suddenly receiving tons of NTP responses to my Web Server”?

This allows you not only to have true visibility, but also can bolster your defences in advance of such attacks and their counter-evolution against our defences.

@drgfragkos



A "Cyber Resilience strategy" has become the next logical step for defending against the unavoidable evolution of threats.

Defence mechanisms need to constantly counter-evolve against the counter-evolution of emerging threats, in order to be able to detect, prevent, respond, recover and further evolve.

This type of constant need for scalability and adaptation becomes even more challenging and demanding when it meets complex systems, which are also high-value targets.

Jump on the cyber-evolution train..

- Move beyond outdated solutions and **ask** the right questions.
- Up to what level **risk** should be considered acceptable?
- Demonstrate **Due Diligence** to avoid claims of negligence.
- Consider **Cyber Insurance** coverage.
- Have a dynamic & equally evolving resilience plan capable of responding to evolving threats which also allows you to **stay within budget**.

Conclusions..

> Cybersecurity Skills Gap? (looking for cyber unicorns?)

> Ticking the Compliance box, does not prevent a potential breach.

> The Dark Web does not have office hours. However, cyber criminals are not smarter that our security experts. Listen to your security professionals and get advice from third parties.

> Make it difficult for cyber criminals to target you (for "fun" or "profit").

> You know the complexity of your systems way better that any attacker.
Use this to your advantage.

> Reputation damage vs Fines

BALCCON2K17

U CNT CTRL ME

Thank you for your attention.

Follow @drgfragkos