

Leadership Failures Behind Major Cyber Breaches

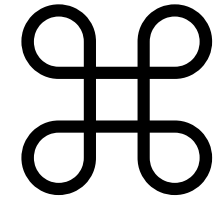


by Todor Todorov

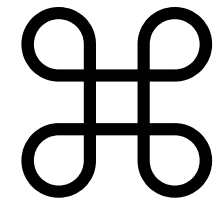


```
todor@AIBEST:~$ whoami
```

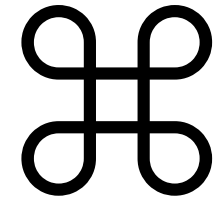
Payhawk



Senior Software Engineer

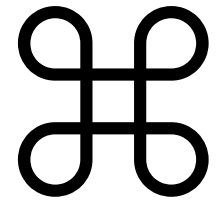


Chapter Leader



Speaker

XAKEP.BG



Community Supporter



The exploit may be technical.
The damage is often managerial.



```
function(b, f){var g=  
c.promise():this.  
e(b[2][2].lock),e(f  
length,f!==d||a&&n.isFunc  
new Array(d),k=new Ar  
return n.ready.prom  
e(handler&&(n(d).trig  
function K(){(d  
e("onLoad",K  
in n(l))break;l.  
border:0;width:0;  
c.style.zoom=1)  
c?!1:!b||b!==!  
c?!0:"false"==  
"string"!=typeof  
n.camelCase(b)
```

1

EQUIFAX

2

 **TARGET**

3

Uber



```
function(b,f){var g=
==d?c.promise():this.
le,b[2][2].lock),elf
f!|=d||a&&n.isFunc
new Array(d),k=new A
return n.ready.prom
handler&&(n(d).trig
)}function K(){(d
attachEvent("onload",K
for(l in n(l))break;l
border:0;width:0;
(c.style.zoom=1)
!|=c?!1:|b||b!|=
!|=c?!0:"false"==
"string"!=typeof
(n(n.camelCase(b))
```

EQUIFAX

Before the breach

Leadership tolerated a known or knowable exposure and lacked evidence that the control was actually working.



Story

- ◎ Attackers exploited a known Apache Struts vulnerability.
- ◎ The FTC said Equifax failed to patch after being notified months before.
- ◎ Leaked names, birth dates, Social Security numbers, and other personal data affecting roughly 147 million people.

EQUIFAX

What leaders should ask instead?

How do we know our most dangerous internet-facing exposures are truly closed?

What evidence do we review when a critical fix is overdue?



1

EQUIFAX

2

 **TARGET**

3

Uber



```
function(b,f){var g=
==d?c.promise():this.
le,b[2][2].lock),elf
f!|=d||a&&n.isFunc
new Array(d),k=new A
return n.ready.prom
handler&&(n(d).trig
)}function K(){(d
attachEvent("onload",K
for(l in n(l))break;l
border:0;width:0;
(c.style.zoom=1)
!|=c?!1:|b||b!|=
!|=c?!0:"false"==
"string"!=typeof
(n.camellase(b))
```



During the breach

Signals existed, but escalation paths and decision rights were too weak to force decisive containment.



Story

- © Attackers entered through a third-party vendor and moved toward payment-card systems during the holiday shopping season.
- © U.S. Senate and Reuters both said Target missed multiple opportunities to stop the breach.
- © The issue was the absence of decisive operational response when the signals were already there.



What leaders should ask instead?

Who can authorize disruptive containment when a critical system is at risk?

What vendor access paths could still let attackers pivot into crown-jewel systems?





“An alert nobody owns is just expensive noise.”



1

EQUIFAX

2

 **TARGET**

3

Uber



```
function(b,f){var g=
==d?c.promise():this.
le,b[2][2].lock),elf
f!|=d||a&&n.isFunc
new Array(d),k=new A
return n.ready.prom
handler&&(n(d).trig
)}function K(){(d
attachEvent("onload",K
for(l in n(l))break;l
border:0;width:0;
(c.style.zoom=1)
!|=c?!1:|b||b!|=
!|=c?!0:"false"==
"string"!=typeof
(n(n.camelCase(b)
```

Uber

After the breach

Trust collapses when leadership treats disclosure and response as optics instead of governance.



Uber

Story

- © Attackers stole data tied to approximately **57 million** Uber users and **600,000** driver license numbers.
- © U.S. Department of Justice said the incident was concealed while Uber was already under FTC scrutiny for its security practices.
- © The case became a governance scandal because leadership choices after the breach amplified the damage and destroyed trust.

What leaders should ask instead?

How do legal, security, privacy, and communications make disclosure decisions in the first 12 hours?

What would stop us from hiding facts to protect optics?

Uber

*“A breach can be survivable.
A cover-up can redefine the company.”*



1

EQUIFAX

2

 **TARGET**

3

Uber



```
function(b,f){var g=
==d?c.promise():this.
le,b[2][2].lock),elf
f!|=d||a&&n.isFunc
new Array(d),k=new A
return n.ready.prom
handler&&(n(d).trig
)}function K(){(d
attachEvent("onload",K
for(l in n(l))break;l.
border:0;width:0;
(c.style.zoom=1)
!|=c?!1:|b||b!|=
!|=c?!0:"false"==
"string"!=typeof
(n.camellase(b))
```

The exploit changes. The leadership failure pattern does not.



Cyber maturity is not just about tools, teams,
or compliance checklists.

- ❑ Leadership attention
- ❑ Governance
- ❑ Escalation
- ❑ Accountability



**NIS2 turns cyber
from an IT topic
into a
management-
body duty.**



What it is

The EU's updated cybersecurity directive, creating a unified framework across 18 critical sectors.

What it demands

Risk management, supply-chain security, incident handling, business continuity, and significant-incident reporting.

What management must do

Approve cyber risk-management measures, oversee implementation, and ensure the organization can prove governance is real.



What executives should do differently now

01 Know the crown jewels

Which systems, processes, and data assets would create existential damage if compromised?

02 Track a few real indicators

Critical risks overdue, MFA coverage, privileged-access hygiene, unresolved high-risk findings, containment time.

03 Assign named executive ownership

Every major cyber risk needs an owner, due date, exception path, and escalation trigger.

04 Rehearse incident decisions

Not just technical tabletop exercises — executive rehearsals for hour-one decisions and disclosure.

05 Demand evidence

Ask how the control is verified in reality, not whether a policy exists in theory.



Attackers may trigger the breach.
Leadership decides whether it becomes a disaster.



Thank you !



@totollygeek

Sources:

- © FTC — Equifax case & settlement
- © U.S. House Oversight Committee — Equifax Report
- © Reuters — Target breach / warning signs
- © U.S. DOJ — Uber breach concealment case
- © European Commission: NIS2
- © EUR-Lex — Directive (EU) 2022/2555
- © Pexels — background / stock images

