SANS European Security Awareness Summit

Once upon a time: Back to the future of security

David Porter, Head of Innovation, Security & Privacy Division, 29 November 2018
Caveat

• Nothing in this presentation represents Bank of England guidance or policy in any way, shape or form

• All opinions expressed are my own
safe and secure
multiple protective layers
redundant components
defined protocols
state-of-the-art technology
manual backup
People Still Weakest Link in Government Cybersecurity

Govies show the riskiest behavior in social media use, physical security and mobile computing.
Amanda Ziadeh
Tue, 05/22/2018 - 16:04

Human Error: The Weakest Link in Cyber Security
May 2, 2018
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
why did that incident happen?
are we missing something?
“I sign on at 8am. A lot of things happen during the day. And when I get home in the evening, I realise the day went ok and we didn’t have any disasters…”
only ONE train in EITHER direction at ANY time
has train left tunnel?

train in tunnel

train out of tunnel
Signalman South

STOP

Signalman North

“Train in tunnel”
STOP

“Has train left tunnel?”

“Train out of tunnel”

Signalman South  Signalman North
Signalman South

GO

Signalman North
multiple protective layers
redundant components
defined protocols
state-of-the-art technology
manual backup
“Train in tunnel”
Gregory

Killick

"Has train left tunnel?"

Scott

"Train out of tunnel"

Hackman

GO

Brown
23 killed
176 seriously injured
AWFUL COLLISION IN CLAYTON TUNNEL.

GREAT LOSS OF LIFE.

The quietude of the town of Brighton was, on Sunday last, alarmingly broken in upon by the occurrence, at a short distance on the main line of Railway, of an accident of a most appalling nature, the like of which has never before occurred on this or, with one exception, any other line of railway in the kingdom. The sensation it created was the more profound from the rarity of accidents of any description on the Brighton line, which is allowed to be one of the best conducted in the whole kingdom.
“Blame Henry Killick”
“Blame Henry Killick”
“Blame Legg”
Brown?
Scott?
Protocol?
Policy?
Signal?
“It is quite clear that the main cause of this accident was not the mistake of the signalman, but the defects of the system under which he worked”
f(i) → f(i,t,c,p,r)
SEQUENCE
repeated protocol messages

DIRECTION
sudden train reversal

TIMING
rapid departure frequency
train reversal
rapid departure
frequency
repeated protocol
messages
flawed protocol
holiday policy
psychophysical fatigue
poor decision making
no logbook
signal failure
We Don't Make Mistakes
We Do Variations
“I sign on at 8am. A lot of things happen during the day. And when I get home in the evening, I realise... But I don’t know why.”
why did that incident happen?
why don’t incidents generally happen?
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
I must follow the rules
I must spot resonances
I must spot resonances
I must spot resonances
I must spot resonances
I must spot resonances
I must spot resonances
I must spot resonances
I must spot resonances
I must spot resonances
I must spot resonances
safe and secure?
1. People are the weakest link — but not the ones you think
2. Don’t fixate on bad — model the good
3. You can’t beat a good story
Thank you