Psychology of Cyber Security

Introduction

The human interaction with computers and technology with regards to cyber security is a complex topic that deserves more attention. In this paper we discuss the psychology of cyber security from a number of different angles. We use real world examples to highlight flaws and to offer solutions for better working practises. The real problem is that humans, especially Government and Corporate level humans are not very keen on admitting mistakes.

The COVID-19 Pandemic will see many countries in the near future demand an inquiry into the appalling amateurish and inadequate response. The report will take 20 years to be published and will be a whitewash, if the UK standard is followed. It will be no one's fault. This seems to be the pattern with Cyber Security. In the case of Boeing, the pilot can always be blamed, you will be flying a 737 Max soon. Good luck.

Oh, what a tangled web we weave,
When first we practise to deceive!

SIR WALTER SCOTT.

Tick-Box Culture

Situation - A large scale government network, before being allowed to open for business, requires a penetration test to ensure compliance with the latest NIST standards,

Task - The project manager is tasked with engaging with an accredited independent penetration test company to ensure that the test occurs and is passed.

Action - The penetration test is conducted. The test is “passed” with a number of corrective remedial actions. A waiver is agreed with the CISO and a date set for the fixes to be implemented.

Result - The box has been ticked. All parties are satisfied and the new network is opened for business as planned.

What really happened?

The scheduled opening of the new network has been published. It is already 12 months late, the new date is cast in stone. No party can afford to be the one seen or deemed to be the one causing the delay. It is too big to fail.

The accredited independent penetration test company is the preferred supplier of the engaging company. In no way will it jeopardise this lucrative relationship. The penetration testers actually only perform a vulnerability scan. This only occurs after they have been given complete access including password to the network. The time, cost, complexity and possible disruption of a real penetration test omits it from consideration. The government hierarchy has no idea what the difference is between a real penetration test and a vulnerability scan.

The difference is carefully omitted from the details of the test and is marketed as a penetration test. Just to ensure that the test meets muster another independent auditor acting on behalf of the government is employed. This gives plausible deniability later down the line, if in the unlikely event a breach occurs, which would result in buck passing. Again the auditor does not want to jeopardize the lucrative contract by being “awkward”.

The financial industry has struggled for decades with the close relationship between the companies and the auditors. There have been many recent cases where companies and given a financial health tick in the box, only to go to the wall months later. The regulators lack teeth and are reluctant to make significant changes.

The same situation applies to the cyber security industry but with even less oversight or audit independence. The holes uncovered in the vulnerability scan are never closed, as the tick in the box has already been acquired. There is no incentive to close the holes. It is debated from time to time every six months or so, but it gets pushed down the agenda and priority list.

Groupthink

Situation - The security governance team have identified a gap in the security audit trail of a network device. This is not compliant and leaves the company exposed on a number of levels from contractual obligation to security accountability.

Task - The security team is tasked with finding the root cause and fixing the problem.

Action - The root cause is identified, and a fix is tested in a development environment. The fix is now ready to be applied and tested in a real world environment. The change management process is followed and approved.

Result - At the last minute, the environment owner orders change management to revoke approval for the change indefinitely.

What really happened?

The gap in the audit trail is significant. The environment owner is approached by the security governance team to fix the issue. The environment owner pushes back citing all sorts of irrelevant business and technical issues. The governance team then approaches the security team, who take the correct approach and attempt to fix the issue. The environment owner hears of the fix at the last minute and instructs the change management team to revoke the approval. The change management team is one hundred strong and not one person had objected to the fix being applied. This seems reasonable given the strict security requirements, which seems the audit trail no complaint. One strong voice has managed to overturn the decision making of one hundred professional people, without providing any coherent, logical or technical reason. When challenged, the reasons given again are weak in fact and reason, but seem enough to confuse and delay the situation.

Behind the scenes, the reason for the delay is simple enough. The strict change management controls are not being adhered to as they are costly and cumbersome. Unauthorised changes are being made all the time. This is advantageous for the environment owner, as it means his team can avoid the time and expense of going through the change management process. They can make changes during normal working hours, again reducing costs. When things go wrong, his team avoids scrutiny and blame, there is no record of the changes, changes are denied or blamed on other parts of the network. An audit trail is the last thing they want.

The Groupthink of one team which goes against the best interests of the company as a whole, manages to overpower the other teams within the project for financial gain and to avoid scrutiny. In simple terms it is fraud. Executive management become aware of it but are reluctant to intervene, becoming complicit in the fraud.

Facts not Fiction

Situation - Enigma traffic had been decoded unusually far in advance of a German Blitz in the Midlands. The attack planned for 14 November 1940 code-named Operation Mondscheinsonate (Moonlight Sonata), was intended to destroy Coventry's factories and industrial infrastructure.

Task - The countermeasures organisations were to jam the X-Beams that guided the German bombers.

Action - R.V. Jones of the Intelligence Section had successfully guessed the frequencies of the German blitz, and this was given to the countermeasures organisation to Jam the signals. The Enigma codes were not decoded in time on this occasion to confirm the frequencies.

Result - The countermeasures organisations claimed success in jamming the X-Beams.

What really happened?

An estimated 568 people were killed in the raid (the exact figure was never precisely confirmed), with another 863 badly injured and 393 sustaining lesser injuries.
X-Gerät (X-Apparatus) had been captured from a german aircraft that had been shot down. Once examined it was determined that the filter was tuned to 2000 cycles per second top “C” on a piano.

The British jammers had been set to 1500 “G” below top “C”. The frequencies had been guessed correctly and later Enigma decodes proved this. The difficult parts had been taken care of, but a seemingly trivial detail was missed. Whoever made such an error ought to have been shot. No one else checked the measurements. An argument ensued with the countermeasures team claiming that the Germans had switched from 1500 to 2000 to foil the jamming. This was proven to be impossible otherwise the change in modulation of the German beams would have been detected. The Germans had always been using 2000.

Even worse was the claim of successes of jamming the X-beams. There was no evidence for this in either the Enigma traffic decodes or in the fact that the German had failed to find their targets. The officers were kidding themselves, not for the first time it was wishful thinking.

R.V. Jones was not a popular man for pointing to the facts. Senior officers tried to suppress his criticisms. Thankfully Churchill recognised the genius of Jones, and his work was a fundamental part of winning the “Battle of the Beams”.

The full story can be read in “Most Secret War” R.V. Jones. This book contains many brilliant examples from the war which are relevant to the psychology of cyber security.

Strategic Ambiguity

Situation - A problem has been detected with TLS comms to a third party. All other TLS comms to other parties are working correctly.

Task - The security team is tasked with investigating the problem and finding the root cause.

Action - The root cause is identified as a vendor A specific problem to another vendor B specific device. The TLS1.2 protocol is not being correctly followed by the vendor A device and a support ticket is raised.

Result - A workaround is suggested and this is tested with the live customer environment. It is successful. The support ticket is closed.

What really happened?

Vendor A at first refuses to accept that the issue is with their kit and points to vendor B as being the culprit. When evidence is supplied to Vendor A, the strategic ambiguity machine kicks in. Vendor A points to support level contracts clauses, software release cycles and support policies. The wording is deliberately ambiguous and contradictory. It is very difficult to replicate the issue without the Vendor B kit being the server and Vendor A being the client. However the wireshark traces show the issues clearly and this is eventually accepted after months of wrangling.
Vendor A wants to avoid providing a fix for v1.0. This would be very time consuming, complicated and costly. Instead it provides a workaround and proposes that the fix will be available in v2.0 within 6 months. In fact the fix was not available until v4.0, two years later.

Only the software industry seems to be able to work in this manner. Sell a solution. Refuse to even talk about any issues until a support contract has been purchased. Obfuscate the problem and hide behind a wall of deliberate ambiguity. Refuse to accept any responsibility for issues, use the clients as live guinea pigs to help fix and improve the software and then force the client to purchase an upgrade along with a support contract.

Anomaly Detection

Situation - Post Office Ltd launched a new IT system called Horizon. In 2013 the system was being used by at least 11,500 branches, and was processing some six million transactions every day. Problems with the system were first reported by Alan Bates, the sub-postmaster at Craig-y-Don, in around 2000.

Task - Fujitsu who designed Horizon at a cost of £1 billion were tasked with finding out why there were so many accounting anomalies being reported.

Action - Fujitsu discovered that the anomalies were due to theft and fraudulent activities at sub-postmaster branches.

Result - The thieves were taken to court and the rule of law took its course resulting in convictions. Stolen monies were ordered to be repaid plus fines and some went to prison. Justice was served.

What really happened?

The Horizon system was designed by idiots, written by imbeciles and tested by morons. It was not fit for purpose. The Horizon system had zero data integrity. The shocking problem was that it took nearly 20 years for this to be officially recognised by the courts.

Fujitsu when initially tasked with finding the root cause of the accounting anomalies acquired a HAL mentality. “Horizon is the most reliable computer system ever made. The Horizon system has never made a mistake or distorted information. It is by any practical definition of the words, foolproof and incapable of error.”

The most frightening aspect of this case is that the Post Office and Fujitsu managed to convince the police, the judiciary and juries that Horizon is perfect; therefore, any accounting anomalies were due to fraudulent activity. Little old ladies were sent to prison on this premise. People lost they homes, livelihoods, reputations, spent time in prison and in at least one case commited suicide.

After the subpostmasters won the court battle, which vindicated them and
implicated the Post Office with serious failures, their fight for justice continued. Pressure is being put on politicians with calls for the legal costs of subpostmasters to be paid by the government and the launch of a judge-led public inquiry.

Subpostmasters were awarded £57.75m in damages, but after costs were taken out they were left with around £10m, which means subpostmasters will not even get back the money they lost. There are also calls for the people responsible for allowing the scandal to happen to face justice.

Data Integrity

Situation - The year is 2020. A global pandemic called COVID-19 is sweeping across the globe killing hundreds of thousands.

Task - The collection of data, everything from symptoms, to deaths and preventative medicine is paramount to combating the virus.

Action - One company called Surgisphere Corporation submits a paper to The Lancet on the topic of Hydroxychloroquine with respect to treating COVID-19.

Result - The Lancet published the study which found no benefit to COVID patients after taking the drug. This was significant as President Trump himself had been touting the benefits of taking Hydroxychloroquine and revealed he was taking it himself. Now it was official, there was no medical benefit, in fact patients taking Hydroxychloroquine were more likely to die in hospital, and prompted the World Health Organization to halt global trials of the drug to treat COVID-19.

What really happened?

Surgisphere Corporation, a tin pot operation saw the dollar signs and wanted to be at the forefront of a new dawn in fast data mining. They had managed to convince the world's leading medical journal that it had a "rapid diagnostic tool" enabling it to swarm the available medical data sets from across the world. The only problem was that no hospital had heard of this company and none had handed over any data. The integrity of the data was questioned. The Guardian revealed that several of Surgisphere's employees had “little or no scientific background; one employee appeared to be a science fiction author while another, listed as a marketing executive, was an adult model.” The Lancet had been duped.

On 4 June, 2020, The Lancet retracted the study, as did the NEJM. The WHO resumed its hydroxychloroquine drug trials.

It is no wonder that crooks want to cash-in on the pandemic. It is also no surprise that the Lancet was asleep at the wheel, as is so often the case with many organisations that we should trust. To be fair they retracted the study, how many other cases like this have slipped through the net?