TEKTUT

FREE GUIDE

5 Cyber Attacks That Changed Everything

Real breaches. Real consequences. And why the people who stop them are more in demand than ever.

TRUE STORIES | REAL IMPACT | CAREERS IN FOCUS

Cyber security can sound like an abstract concept — firewalls, encryption, threat vectors. But every now and then, the real world reminds us exactly what's at stake. People's secrets exposed. Hospital equipment held hostage. Industrial machinery destroyed by a piece of code no one could see. These aren't sci-fi plotlines. They happened. And they keep happening — which is precisely why the people who prevent them are so valuable.

Here are five of the most significant cyber attacks in recent history, broken down by the consequences they caused — and what they tell us about the world we're all living in.

CASE 01

Ashley Madison

Consequence: Reputation & Personal Destruction

37M	2015	2
accounts exposed	year of breach	executives resigned

Ashley Madison was a dating website with a very specific purpose: helping people have affairs. Their marketing tagline was, famously, "Life is short. Have an affair." Which is bold. Arguably too bold, as it turns out.

THE BREACH

In 2015, a hacking group called The Impact Team broke in and demanded the site shut down. When it didn't, they released the personal data of 37 million users — names, email addresses, sexual preferences, home addresses, and payment details. All of it. Online. For anyone to search.

Here's where it gets particularly uncomfortable: a lot of those email addresses were work addresses. Government employees. Military personnel. Clergy. People who had presumably not told their spouses they were on the site — and were now very publicly findable by anyone with a browser.

The human cost was severe. Reported suicides were linked to the exposure. Divorces followed. Careers ended. Extortion attempts flooded inboxes within days of the dump. The company's CEO resigned. A second executive resigned shortly after. The business — which had been planning a £200M IPO — was effectively finished as a credible brand.

And here's the kicker: Ashley Madison had been charging users a fee to delete their data. A paid deletion service. That didn't delete the data. Not only were the users' details still sitting in the database — the attackers made sure everyone knew they'd paid for a service that was essentially fiction.

WORTH NOTING

It's very hard to feel sorry for people who were caught cheating. But that's rather the point — once data is out, it can be used to hurt anyone, regardless of whether you think they deserve it. The weaponisation of personal data doesn't come with a moral filter.

THE ANALYST'S LESSON

This is a textbook case for why data minimisation and proper deletion processes matter. Organisations that hold sensitive personal data have a duty to protect it — and to actually delete it when asked. A GRC Analyst or Data Protection Officer reviewing Ashley Madison's practices beforehand could have flagged both the retention failure and the deceptive deletion feature as critical risks. They weren't reviewed. Nobody stopped it.

CASE 02

Florida Water Treatment Plant

Consequence: Public Safety — Near Miss

111x	2021	15,000
sodium hydroxide increase attempted	year of attack	residents at risk

In February 2021, an operator at a water treatment plant in Oldsmar, Florida, was sitting at his desk when he noticed something odd. His cursor was moving — by itself. Someone had remotely accessed his computer and was clicking around the plant's control systems.

THE BREACH

The attacker navigated to the controls for sodium hydroxide — the chemical used to adjust water pH. A safe level is around 100 parts per million. The attacker attempted to change the level to 11,100 parts per million. That's lye. The kind that causes chemical burns. The kind that would have poisoned the water supply for around 15,000 people.

The operator caught it in real time and reversed it immediately. A near miss — but a near miss that should stop all of us in our tracks for a moment.

Because here's the thing we rarely think about: we trust infrastructure completely. When you turn on the tap, you don't test the water. You don't verify the chemical balance. You just assume that somewhere, someone — or something — is keeping it safe. And that something is increasingly digital. Increasingly networked. Increasingly accessible to anyone with a laptop and the right credentials.

The Oldsmar plant was running Windows 7 — an operating system Microsoft had stopped supporting over a year earlier. Remote access was enabled via TeamViewer, with no firewall and a shared password across all staff. This wasn't a sophisticated attack. It required no great skill. It just required someone to try.

WORTH NOTING

Critical national infrastructure — water, power, hospitals, transport — is increasingly connected to the internet for efficiency. That connectivity is also an attack surface. The question isn't whether attackers will try to exploit it. They already are.

THE ANALYST'S LESSON

A basic security audit would have caught every single vulnerability in Oldsmar: end-of-life OS, shared credentials, no MFA, unrestricted remote access. Patch management and access control aren't glamorous topics — but they are, quite literally, the difference between safe drinking water and a public health emergency. This is exactly the kind of risk a Cyber Analyst or SOC team exists to find and close.

CASE 03

Stuxnet

Consequence: Geopolitical & Infrastructure Sabotage

~1,000	2010	5 years
centrifuges destroyed	discovered	estimated development time

If the previous two cases made you uneasy, Stuxnet is the one that changes how you think about cyber security entirely. Because Stuxnet wasn't about stealing data, or making money, or embarrassing anyone. It was a weapon. A real one. Designed, built, and deployed by a nation state — widely attributed to the US and Israel — to physically destroy another country's nuclear infrastructure.

THE BREACH

Stuxnet targeted Iranian uranium enrichment facilities — specifically the centrifuges used to enrich uranium at Natanz. It spread via USB drives, infected Windows machines, and then lay dormant — waiting. When it detected the exact industrial control system used by those centrifuges, it made them spin at the wrong speed. Just wrong enough to destroy themselves. While simultaneously reporting back to the operators that everything was perfectly fine.

Read that again. The machines were destroying themselves, and the engineers watching the monitoring screens saw nothing unusual. The malware had compromised the readouts too. Around 1,000 centrifuges were physically wrecked before anyone understood what was happening.

Stuxnet is considered the world's first known cyber weapon — the moment the world moved from cyber crime into cyber warfare. It proved that a piece of code, given enough time and sophistication, could cause physical destruction on the scale of a military strike. No soldiers. No missiles. Just software.

When it was eventually discovered and analysed, it had roughly 15,000 lines of code — an extraordinary level of complexity for malware at the time. Security researchers called it unlike anything they had ever seen.

WORTH NOTING

Stuxnet escaped. It was designed to target a very specific system — but it spread via USB drives and infected machines worldwide. The weapon got loose. That's a recurring theme with cyber tools: once they exist, they're very hard to contain.

THE ANALYST'S LESSON

Stuxnet is why the phrase 'Threat Intelligence' exists as a career specialism. Understanding not just what attackers do, but who they are, what they want, and what tools they're using — that's the job of a Threat Intelligence Analyst. The MITRE ATT&CK; framework that analysts use today was built in direct response to attacks like Stuxnet. The sophistication of the threat drove the sophistication of the defence.

CASE 04

British Airways

Consequence: Regulatory Fine & Financial Fallout

500K	£20M	2019
customers affected	ICO fine	year of ruling

In 2018, British Airways suffered a data breach that affected around 500,000 customers. Attackers had injected malicious code into the BA website — specifically the booking page — that harvested payment card details and personal information as customers typed them in. It ran undetected for over two months.

THE BREACH

The technique is called 'skimming' or a 'Magecart attack' — a small piece of malicious JavaScript sitting quietly on a payment page, silently copying everything a user types and sending it to the attacker's server. BA's security monitoring failed to detect it for 58 days.

When GDPR came into force in 2018, it gave regulators real teeth. The Information Commissioner's Office (ICO) investigated and found that BA had failed to implement adequate security measures — and fined them £20 million. That's not a cost of doing business. That's a boardroom conversation. That's executives losing sleep.

The original proposed fine was actually £183 million — nearly 1.5% of BA's global turnover. It was reduced significantly due to the economic impact of COVID-19 on the airline industry. Even so, £20 million. For a breach that could have been caught with proper monitoring.

The reputational cost is harder to quantify but arguably worse. Customers whose payment details were stolen don't forget. Trust, once lost, takes years to rebuild — if it comes back at all.

WORTH NOTING

GDPR changed the calculus entirely. Before 2018, a breach might cost a company some PR headaches and a modest payout. After GDPR, it can cost a percentage of global annual turnover. Suddenly 'we'll deal with security later' stopped being a viable business strategy.

THE ANALYST'S LESSON

This is a GRC and SOC story. A GRC Analyst would have ensured GDPR compliance frameworks were in place before the breach. A SOC team with proper monitoring would have detected the anomalous data exfiltration within hours, not months. The £20M fine represents roughly what it would cost to employ a dedicated security team for many years. The maths is not complicated.

CASE 05

WannaCry & the NHS

Consequence: Operational Shutdown & Human Cost

£92M	19,000	80
cost to NHS	appointments cancelled	NHS trusts affected

In May 2017, a ransomware attack called WannaCry tore through organisations in over 150 countries. It encrypted files on infected machines and demanded a Bitcoin payment to unlock them. Hundreds of thousands of machines were hit in a matter of hours. Among the hardest hit: the UK's National Health Service.

THE BREACH

WannaCry exploited a vulnerability in Windows called EternalBlue — a tool originally developed by the NSA that had been leaked online weeks earlier. It spread automatically across networks without anyone clicking anything. NHS trusts running unpatched, end-of-life Windows systems were completely defenceless.

Here's what that actually meant in practice: doctors couldn't access patient records. MRI scanners went offline. Blood test results couldn't be retrieved. Ambulances were diverted away from A&E; departments because hospitals couldn't safely accept patients. Nineteen thousand appointments and operations were cancelled.

Think about that. A patch — a free software update that Microsoft had released two months earlier — was the difference between those appointments happening and not happening. Between patients receiving care and being turned away. We rely on the NHS not just with our health, but with our lives. And the NHS relies on technology. Technology that, in 2017, included thousands of machines running Windows XP — an operating system Microsoft had stopped supporting in 2014.

The £92 million cost to the NHS came from IT recovery, lost output, and the enormous effort of cleaning and rebuilding infected systems. That's money taken directly away from patient care. From wards. From staff. From equipment.

WORTH NOTING

WannaCry was stopped — accidentally — by a 22-year-old security researcher named Marcus Hutchins, who noticed the malware checked a specific domain before spreading and registered it for £8. That domain registration acted as a kill switch. One person, one domain, £8 — and one of the largest cyber attacks in history was slowed. Security is a human endeavour.

THE ANALYST'S LESSON

WannaCry is the clearest possible argument for patch management and asset inventory. Knowing what systems you have, what OS they run, and whether they're up to date is not glamorous work — it's the kind of thing that gets called 'hygiene'. But unpatched systems killed WannaCry's victims. A Cyber Analyst running a basic vulnerability scan would have flagged every single one of those EternalBlue-vulnerable machines. The fix was free. The failure to apply it cost £92 million.

So What Does This Mean For You?

Every case in this guide has something in common: a human being, somewhere, either failed to act — or wasn't there to act at all.

Ashley Madison needed someone to enforce proper data deletion policies. Oldsmar needed someone to patch a years-old OS and lock down remote access. Stuxnet needed analysts who understood how nation-state threats operate at an industrial level. British Airways needed a SOC team that could detect anomalous traffic on a booking page. The NHS needed someone to run a vulnerability scan and say — months earlier — "these machines need updating, now."

That person is a Cyber Security Analyst. A GRC Specialist. A SOC Engineer. A Threat Intelligence professional. These are not niche, exotic roles. They are foundational — and they are in short supply.