Cyber warning for prisons

A government watchdog has warned that Scotland's prisons are vulnerable to cyber attacks by criminal hackers due to poor online security.

Scotland's Auditor General has told the Scottish Prison Service (SPS) that a cyber attack could "significantly impact" both its finances and operation.

The public sector spending watchdog says SPS needs to be better prepared should "an attack or disaster occur" amid continuing "significant risks of cyber attacks to public bodies".

The SPS's 2022/23 Annual Audit Report said the risk made it "even more important" that the SPS ensures it has "appropriate policies and procedures in place".

It warned SPS risked not being sufficiently protected against "common online threats" and also advised they should "ensure they have appropriate independent cyber accreditation".

It recommends: "With the ever growing cyber risks faced, SPS should ensure that it is meeting the minimum requirements set out in the Public Sector Cyber Resilience Framework (PSCRF)."

The warning comes despite the SPS having already fallen victim to international hackers who targeted its website in January 2021.

Online criminals claiming to be linked to Morocco knocked the webpage offline for around an hour after they replaced normal

content with a message saying “hacked by Morocco Hack Team”.

Prison chiefs launched an urgent investigation after the attack was detected at around 11am and the website was restored an hour later.

It has also emerged the SPS was rejected for two government-backed cyber security schemes – Cyber Essentials, an industry scheme helping organisations protect themselves against common online threats and for Public Services Network (PSN) accreditation.

According to the auditor’s report, PSN compliance is a way to report security arrangements and is “how a public body demonstrates that their organisation’s security arrangements, policies and controls are sufficiently rigorous for the Cabinet Office to allow the public sector body to interact with the PSN and those connected to it”.

The report says: “Cyber Essentials is a government-backed, industry-supported scheme that helps organisations protect themselves against common online threats. The base certification is a self-assessment that ensures protection against a variety of the most common cyber-attacks.

“Cyber Essentials is also a requirement under the Public Sector Cyber Resilience Framework (PSCRF). SPS were unsuccessful in their application for Cyber Essentials accreditation.”

The report adds: “SPS has also been rejected for Public Services Network (PSN) accreditation. PSN compliance is a way to report security arrangements.

“It is how a public body demonstrates that their organisation’s security arrangements, policies and controls are sufficiently rigorous for the Cabinet Office to allow the public sector body to interact with the PSN and those connected to it.

“With the ever growing cyber risks faced, SPS should ensure that it is meeting the minimum requirements set out in the Public Sector Cyber Resilience Framework (PSCRF).”

A spokeswoman for the SPS said: “SPS is currently taking steps to gain accreditation of Cyber Essentials, as we are with meeting the minimum requirements of the Public Sector Cyber Resilience Framework.”