

Ransomware Prevention & Mitigation

## 9-Point Ransomware Readiness Assessment

**Cyber attackers can knock out companies in an instant using the latest ransomware technologies, leaking internal information, corrupting data, and demanding ransoms. Best-case scenario, such an attack results in poor PR headlines or production stops. Worst-case, your company's existence is on the line. It's time to prepare: Our 9-Point Ransomware Readiness Assessment reveals your IT's hidden vulnerabilities and security weaknesses**



Your IT is now more vulnerable than ever: hybrid work, cloud solutions and a spread-around-the-globe workforce make your business far more flexible but put it in the crosshairs of cyber attackers. Ransomware protection is becoming a must-have component of any IT's security to avoid outages or loss.

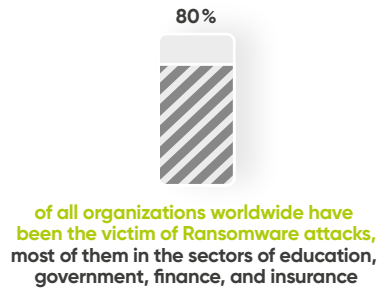
Following the 2020 pandemic's dramatic increase in remote work, Swiss IT Security AG saw an even more dramatic rise in ransomware incidences among new clients. We acted fast to protect existing and new clients: Our **9-Point Ransomware Readiness Assessment** is based on years of experience dealing with Ransomware. Our experts evaluate your IT infrastructure top-to-bottom to protect against common Ransomware techniques, plug vulnerabilities, and help you eliminate weaknesses before it's too late.



## The Ransomware Threat

**Ransomware** infiltrates your IT in multiple ways, usually through email attachments or downloads. Once executed, it encrypts critical corporate data and locks out all users until the ransom

is settled, usually via Bitcoin or other crypto currencies. In the end, your firm is at the mercy of the attacker. The result can be catastrophic, and the threat is ever-growing:



\*Sources: [www.ibm.com](http://www.ibm.com) | PwC, 2022 Global Digital Trust Insights | [www.netzwoche.ch](http://www.netzwoche.ch)

## Overview

Swiss IT Security AG's Ransomware Readiness Assessment is designed to evaluate the effectiveness of your security measures and ability to quickly react and restore your systems in case of a Ransomware attack.

This framework is based on years of experience dealing with Ransomware incidences from clients', the latest in Ransomware behavioral threat analysis, as well as common practices of renowned IT security bodies around the world. It includes:

## 3 Reasons Why You Should Run a Ransomware Risk Assessment

### CHECK FOR VULNERABILITIES

Our Swiss IT Security Experts check the effectiveness of your security measures against all current tactics, techniques, and procedures of the latest Ransomware attackers. We'll unveil potential vulnerabilities and show which areas of your IT could be exploited by Ransomware.

### EFFECTIVENESS OF YOUR RESPONSE

When disaster strikes, time is of the essence: Our **9-Point Ransomware Readiness Assessment** helps analyze the speed and effectiveness of your countermeasures, preparing you for a swift recovery.

### IDENTIFY IMPROVEMENTS

We evaluate technical risks and operational impacts of Ransomware attacks, helping you set up detailed procedures to both improve your IT and set up a recovery plan.

### Swiss IT Security AG

Etzel matt 3, 5430 Wettingen  
Phone: +41 848 088 088  
info@sits.ch – www.sits.ch



If you need further assistance or have any questions related to the offer, please do not hesitate to contact our team of experts.

## Stay safe with our 9 Point Ransomware Readiness Assessment

Our experts have carefully crafted the “**9-Point Ransomware Readiness Assessment**” for businesses of all sizes to help prevent against Ransomware attacks and prepare for the worst-case scenario. Our systems analyze your ability to act in case of a security incident and help fix vulnerabilities before they become real problems.



## Next Steps: Our Services

Our **9-Point Assessment** is just the beginning: Once the results are in, Swiss IT Security AG can take you to the next level and support you while executing in all areas – from setting up new processes to ongoing maintenance and helping in a crisis:

### Prevention

- ☒ Development of ransomware guidelines and processes as well as risk management and corporate governance.
- ☒ Awareness training for your employees.

### Detection & Forensics

- ☒ Instant analysis and tracing of a ransomware attack
- ☒ Reporting of all impacted systems and setting up concrete emergency steps

### Response & Elimination

- ☒ Removal of **ransomware** and lockdown of all impacted systems
- ☒ **Implementation** of backup & recovery workflows

### Recovery

- ☒ **Setting up** all critical services and systems from the ground up based on top notch security and networking technology.
- ☒ **Resuming** normal operations

Get a tailor-made offer from Swiss IT Security AG today to prevent and restore any Ransomware attack.

### Swiss IT Security AG

Etzel matt 3, 5430 Wettingen  
Phone: +41 848 088 088  
info@sits.ch – www.sits.ch



If you need further assistance or have any questions related to the offer, please do not hesitate to contact our team of experts.