



«I sabati di AICIM»

La Cybersecurity nel processo di digitalizzazione di una PMI

18 marzo 2023
h. 10-12

10.00: Apertura lavori

Gianmarco Biagi, Presidente AICIM-AISOM e Holding 7p9

10.10: consapevolezza e sviluppo della sicurezza informatica nelle PMI

Michele Vanzi, Coordinatore Team Innovazione & ITC,
Founder Michele Vanzi&Partners

10.20: studio ed attuazione di un progetto di sicurezza informatica

Giulio Valeri, Founder Software Solutions S.r.l.

10.35: implementazione di sistemi per la protezione dei dati: aspetti legali ed operativi

Maria Clara Piatti, Innovaton Manager/ **William Di Cicco**, Avvocato

10.55: Le insidie informatiche di oggi e di domani: come difendersi

Giorgio Sbaraglia, Information & Cyber Security Advisor | DPO
| Docente 24 Ore Business School | Comitato Direttivo CLUSIT

11:55: Q&A - conclusione

Giulio Valeri

Membro Comitato Direttivo – Innovazione ICT

<http://www.aisom.it/>

CEO Software Solutions Srl

<http://www.softsol.it/>

Linkedin: <https://www.linkedin.com/in/giulio-valeri-4194403/>



INIZIAMO CON UN PO' DI «NUMERI» RAPPORTO CLUSIT 2022

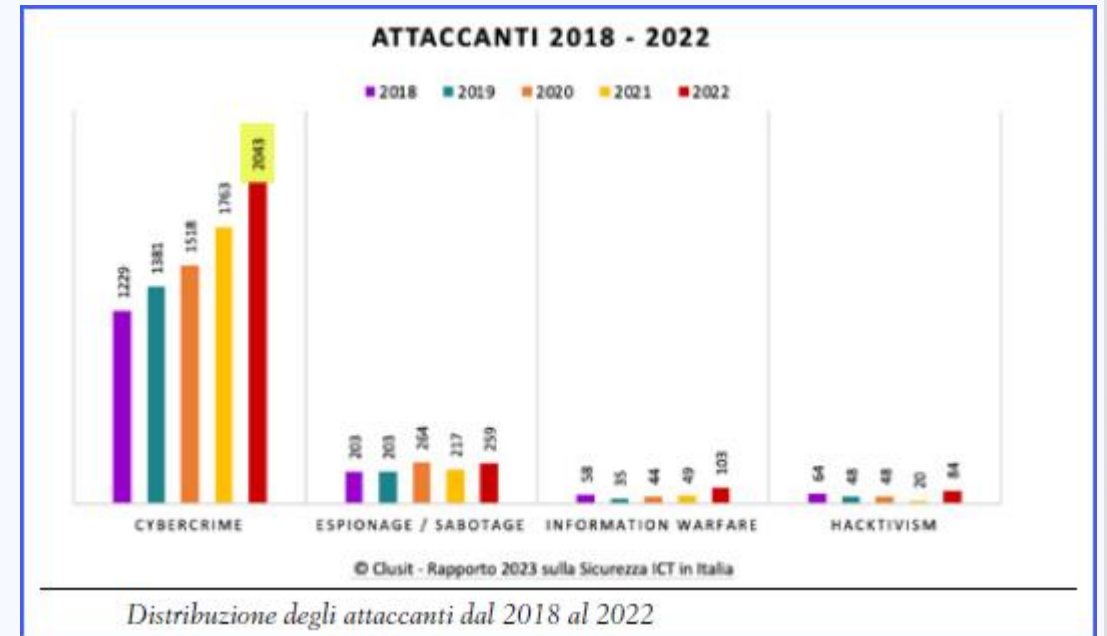
Rapporto
 Clusit

2023

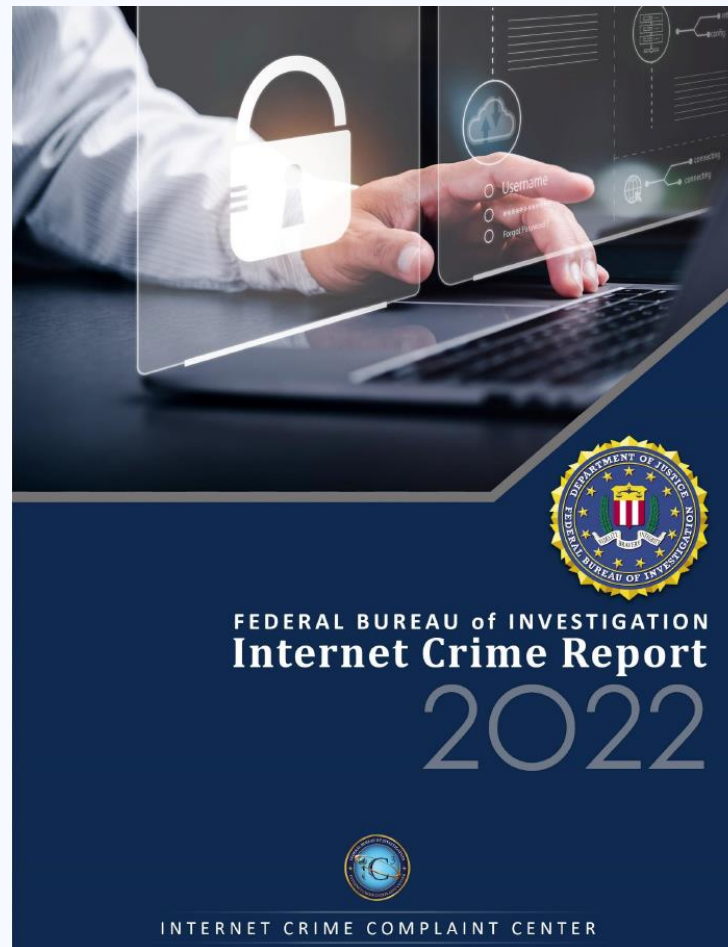
sulla sicurezza ICT
in Italia



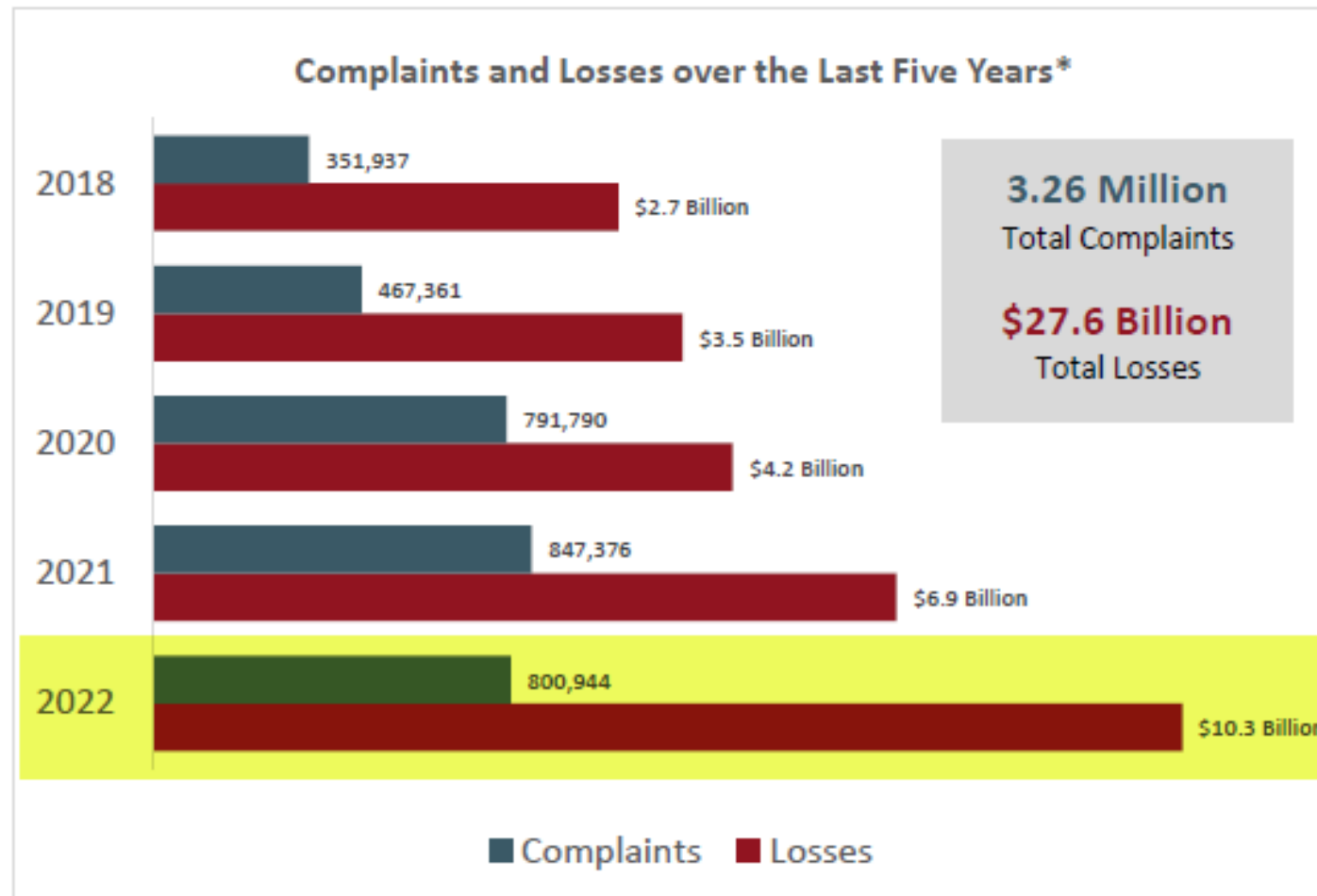
ATTACCHI ANALIZZATI DA CLUSIT: 2.489 NEL 2022



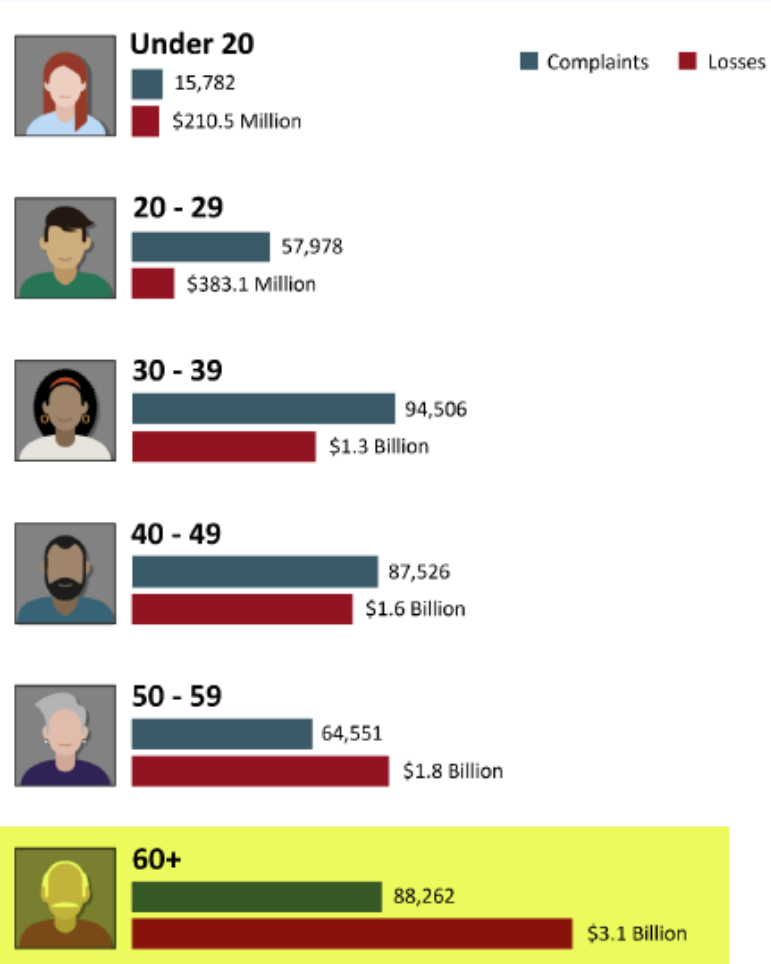
COSA SUCCEDE NEGLI USA: DA FBI – IC3 REPORT 2022



STATISTICA DEGLI ULTIMI 5 ANNI



2022 - VITTIME PER FASCIA DI ETÀ



COMPARAZIONE DEGLI ULTIMI 3 ANNI

LAST THREE-YEAR COMPLAINT LOSS COMPARISON

| By Victim Loss | ▼ ▲ = Trend from previous Year | | |
|---------------------------------|--------------------------------|-------------------|-------------------|
| Crime Type | 2022 | 2021 | 2020 |
| Advanced Fee | \$104,325,444 ▲ | \$98,694,137 ▲ | \$83,215,405 ▼ |
| BEC | \$2,742,354,049 ▲ | \$2,395,953,296 ▲ | \$1,866,642,107 ▲ |
| *Botnet | \$17,099,378 ▲ | N/A | N/A |
| Confidence Fraud/Romance | \$735,882,192 ▼ | \$956,039,739 ▲ | \$600,249,821 ▲ |
| Credit Card/Check Fraud | 264,148,905 ▲ | \$172,998,385 ▲ | \$129,820,792 ▲ |
| Crimes Against Children | \$577,464 ▲ | \$198,950 ▼ | \$660,044 ▼ |
| Data Breach | \$459,321,859 ▲ | \$151,568,225 ▲ | \$128,916,648 ▲ |
| Employment | \$52,204,269 ▲ | \$47,231,023 ▼ | \$62,314,015 ▲ |
| Extortion | \$54,335,128 ▼ | \$60,577,741 ▼ | \$70,935,939 ▼ |
| Government Impersonation | \$240,553,091 ▲ | \$142,643,253 ▲ | \$109,938,030 ▼ |
| *Harassment/Stalking | \$5,621,402 | N/A | N/A |
| Identity Theft | 189,205,793 ▼ | \$278,267,918 ▲ | \$219,484,699 ▲ |
| Investment | \$3,311,742,206 ▲ | \$1,455,943,193 ▲ | \$336,469,000 ▲ |
| IPR/Copyright and Counterfeit | \$4,591,177 ▼ | \$16,365,011 ▲ | \$5,910,617 ▼ |
| Lottery/Sweepstakes/Inheritance | \$83,602,376 ▲ | \$71,289,089 ▲ | \$61,111,319 ▲ |
| Malware | \$9,326,482 ▲ | \$5,596,889 ▼ | \$6,904,054 ▲ |
| Non-Payment/Non-Delivery | \$281,770,073 ▼ | \$337,493,071 ▲ | \$265,011,249 ▲ |
| Other | \$117,686,789 ▲ | \$75,837,524 ▼ | \$101,523,082 ▲ |
| Overpayment | \$38,335,772 ▲ | \$33,407,671 ▼ | \$51,039,922 ▼ |
| Personal Data Breach | \$742,438,136 ▲ | \$517,021,289 ▲ | \$194,473,055 ▲ |
| Phishing | \$52,089,159 ▲ | \$44,213,707 ▼ | \$54,241,075 ▼ |
| Ransomware | \$34,353,237 ▼ | \$49,207,908 ▲ | \$29,157,405 ▲ |
| Real Estate | \$396,932,821 ▲ | \$350,328,166 ▲ | \$213,196,082 ▼ |
| *SIM Swap | \$72,652,571 | N/A | N/A |
| Spoofing | \$107,926,252 ▲ | \$82,169,806 ▼ | \$216,513,728 ▼ |
| Tech Support | \$806,551,993 ▲ | \$347,657,432 ▲ | \$146,477,709 ▲ |
| *Threats of Violence | \$4,972,099 | N/A | N/A |

*New Crime Types added in 2022

LAST THREE-YEAR COMPLAINT COUNT COMPARISON

| By Victim Count | ▼ ▲ = Trend from previous Year | | |
|---------------------------------|--------------------------------|-----------|-----------|
| Crime Type | 2022 | 2021 | 2020 |
| Advanced Fee | 11,264 ▲ | 11,034 ▼ | 13,020 ▼ |
| BEC | 21,832 ▲ | 19,954 ▲ | 19,369 ▼ |
| *Botnet | 568 | N/A | N/A |
| Confidence Fraud/Romance | 19,021 ▼ | 24,299 ▲ | 23,751 ▲ |
| Credit Card/Check Fraud | 22,985 ▲ | 16,750 ▼ | 17,614 ▲ |
| Crimes Against Children | 2,587 ▲ | 2,167 ▼ | 3,202 ▲ |
| Data Breach | 2,795 ▲ | 1,287 ▼ | 2,794 ▲ |
| Employment | 14,946 ▼ | 15,253 ▼ | 16,879 ▲ |
| Extortion | 39,416 ▲ | 39,360 ▼ | 76,741 ▲ |
| Government Impersonation | 11,554 ▲ | 11,335 ▼ | 12,827 ▼ |
| *Harassment/Stalking | 11,779 | N/A | N/A |
| Identity Theft | 27,922 ▼ | 51,629 ▲ | 43,330 ▲ |
| Investment | 30,529 ▲ | 20,561 ▲ | 8,788 ▲ |
| IPR/Copyright and Counterfeit | 2,183 ▼ | 4,270 ▲ | 4,213 ▲ |
| Lottery/Sweepstakes/Inheritance | 5,650 ▼ | 5,991 ▼ | 8,501 ▲ |
| Malware | 762 ▼ | 810 ▼ | 1,423 ▼ |
| Non-Payment/Non-Delivery | 51,679 ▼ | 82,478 ▼ | 108,869 ▲ |
| Other | 9,966 ▼ | 12,346 ▲ | 10,372 ▼ |
| Overpayment | 6,183 ▲ | 6,108 ▼ | 10,988 ▼ |
| Personal Data Breach | 58,859 ▲ | 51,829 ▲ | 45,330 ▲ |
| Phishing | 300,497 ▼ | 323,972 ▲ | 241,342 ▲ |
| Ransomware | 2,385 ▼ | 3,729 ▲ | 2,474 ▲ |
| Real Estate | 11,727 ▲ | 11,578 ▼ | 13,638 ▲ |
| *SIM Swap | 2,026 | N/A | N/A |
| Spoofing | 20,649 ▲ | 18,522 ▼ | 28,218 ▲ |
| Tech Support | 32,538 ▲ | 23,903 ▲ | 15,421 ▲ |
| *Threats of Violence | 2,224 | N/A | N/A |

*New Crime Types added in 2022

PERCHÉ UN'AZIENDA DOVREBBE PROTEGGERSI CON LA CYBERSECURITY?

CI SONO DIVERSI MOTIVI PER CUI UN'AZIENDA DOVREBBE PROTEGGERSI CON LA SICUREZZA INFORMATICA:

- PROTEZIONE DEI DATI SENSIBILI
- EVITARE PERDITE FINANZIARIE
- SODDISFARE I REQUISITI NORMATIVI
- MANTENERE LA FIDUCIA DEI CLIENTI
- PREVENIRE L'INTERRUZIONE DELLE OPERAZIONI



LA SICUREZZA INFORMATICA È ESSENZIALE PER PROTEGGERE LE RISORSE, LA REPUTAZIONE E LA CAPACITÀ DI FARE AFFARI DI UN'AZIENDA NEL PANORAMA DIGITALE ODIERNO.

COME PROTEGGERE UN'AZIENDA CON LA CYBERSECURITY?

LA PROTEZIONE DI UN'AZIENDA CON LA SICUREZZA INFORMATICA È UN PROCESSO COMPLESSO E CONTINUO CHE RICHIEDE UN APPROCCIO A PIÙ LIVELLI PER GARANTIRE LA SICUREZZA E LA PROTEZIONE DELLE RISORSE E DELLE INFORMAZIONI DELL'AZIENDA.

ECCO ALCUNI PASSAGGI CHE UN'AZIENDA PUÒ ADOTTARE PER PROTEGGERSI DALLE MINACCE INFORMATICHE:

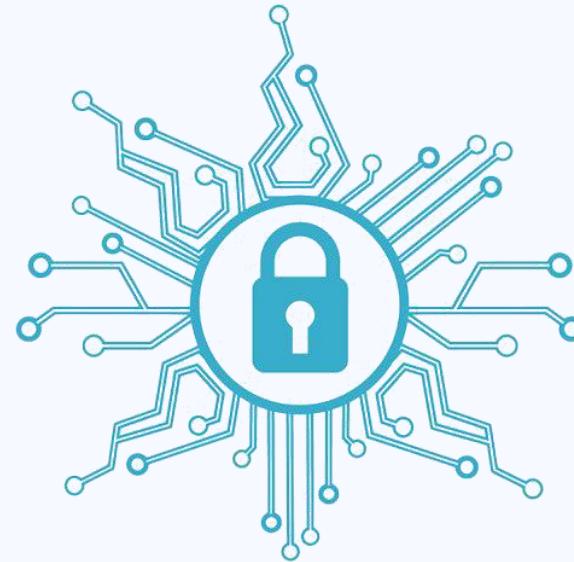


COME PROTEGGERE UN'AZIENDA CON LA CYBERSECURITY?

- CONDURRE UNA VALUTAZIONE DEL RISCHIO APPROFONDATA
- IMPLEMENTAZIONE DI CONTROLLI DI SICUREZZA E TECNICI REGOLARI
- IMPLEMENTARE SEVERI CONTROLLI DI ACCESSO
- IMPLEMENTARE PASSWORD COMPLESSE
- UTILIZZARE L'AUTENTICAZIONE A PIÙ FATTORI
- ESEGUIRE BACKUP REGOLARI
- IMPLEMENTARE LA CRITTOGRAFIA
- IMPLEMENTARE I FIREWALL
- ADOTTARE SOLUZIONI DI CYBERSECURITY
- MANTENERE AGGIORNATO IL SOFTWARE
- FORMARE I DIPENDENTI
- FORNITORI DI TERZE PARTI SICURI
- MONITORARE L'ATTIVITÀ DI RETE
- IMPLEMENTARE UN PIANO DI RISPOSTA AGLI INCIDENTI DI SICUREZZA INFORMATICA

COME PROTEGGERE UN'AZIENDA CON LA CYBERSECURITY?

NEL COMPLESSO, LA SICUREZZA INFORMATICA È UN PROCESSO CONTINUO CHE RICHIEDE MONITORAGGIO, AGGIORNAMENTO E MIGLIORAMENTO COSTANTI. IMPLEMENTANDO QUESTE MISURE, UN'AZIENDA PUÒ RIDURRE SIGNIFICATIVAMENTE IL RISCHIO DI ATTACCHI INFORMATICI E PROTEGGERE LE PROPRIE RISORSE DIGITALI. TUTTAVIA, È IMPORTANTE NOTARE CHE LA SICUREZZA INFORMATICA È UN PROCESSO CONTINUO E LE AZIENDE DEVONO RIMANERE VIGILI E ADATTARSI ALLE NUOVE MINACCE MAN MANO CHE EMERGONO:



LA CYBERSECURITY NON È UNA DESTINAZIONE MA UN PERCORSO...

GRAZIE PER L'ATTENZIONE!

giulio.valeri@softsol.it

www.softsol.it

Mob: +39 3207219660

