NICE VENTURE INFORMATION TECHNOLOGIES LLC

The Cybersecurity Guide for Business

How attacks happen, what every security layer does, the standards that matter, and the first steps every organisation should take.

Book a free security assessment | **Under attack? WhatsApp now**

WhatsApp / call +971 55 134 6136 · sales@nice-venture.com · nice-venture.com

Contents

1. Cybersecurity in plain English
2. The attacks most organisations face
3. What each security layer does
4. What's changing: today's security priorities
5. 10 first steps for every organisation
6. When an attack gets through
7. The standards worth knowing
8. How to choose a cybersecurity partner
9. Glossary
10. Contact us

> Use this guide with your management and IT team. When you want a second opinion, ask us for a free assessment — we score your organisation against these steps and recommend what to fix first.

Cybersecurity in plain English

Cybersecurity keeps your information and systems confidential, accurate and available — so the business keeps running and customers keep trusting you.

Confidentiality, integrity, availability

Only the right people see data, nobody changes it secretly, and systems work when you need them.

Threat, vulnerability, risk

A threat is who could harm you; a vulnerability is the open door; risk is how likely and how damaging an attack would be.

Defence in depth

Several layers of protection, so if one misses an attack, the next one catches it.

Zero trust

Being on the office network no longer means being trusted. Every user, device and request is verified, every time.

People, process, technology

Tools fail without trained people and clear routines. A security programme needs all three.

Shared responsibility in the cloud

Microsoft, AWS and Google secure their platforms. You still own your identities, settings and data.

The attacks most organisations face

Most incidents start with a phishing message, a stolen password or an unpatched system — and end in ransomware, fraud or data theft.

ATTACK	HOW IT WORKS	WARNING SIGNS	WHAT STOPS IT
Ransomware	Attackers get in, steal data, then lock your systems and demand payment.	Files suddenly unreadable, ransom note, backups deleted, admin logins at night.	EDR/XDR, MFA, patching, segmentation, immutable backup, 24/7 monitoring, an incident plan.
Phishing	Fake emails, SMS or WhatsApp messages trick staff into clicking, paying or sharing passwords.	Urgent tone, look-alike sender, unexpected login page.	Email security, awareness training, phishing simulation, MFA, DNS filtering.
Invoice fraud (BEC)	A hijacked or look-alike mailbox changes bank details on an invoice.	A supplier suddenly "changes bank account"; hidden forwarding rules.	MFA, mailbox monitoring, payment call-back checks, DMARC.
Account takeover	Stolen or guessed passwords are used to log in to Microsoft 365, VPN or cloud.	Logins from new countries, repeated MFA prompts.	Phishing-resistant MFA, conditional access, privileged access management.
Insider threat	An employee or contractor leaks or steals data, deliberately or by mistake.	Large downloads, USB copying, access outside their role.	Least privilege, DLP, insider-threat monitoring such as Data Resolve inDefend.
Supply-chain attack	A trusted supplier, software update or IT provider is used to reach you.	Unexpected changes after an update; news of a vendor breach.	Vendor risk reviews, limited vendor access, EDR, application control.
Unpatched systems	Attackers scan the internet for firewalls, VPNs and websites missing updates.	New admin accounts, web shells, firewall alerts.	Vulnerability management, monthly patching, web application firewall.
Web & API attacks	Bots and injection attacks target websites, booking engines and apps.	Spikes in failed logins or odd traffic.	WAF, bot protection, secure development (OWASP), penetration testing.
DDoS	Your website or network is flooded until it stops responding.	Site slow or down; bandwidth saturated.	Cloud DDoS protection and CDN.
Building & OT attacks	Cameras, BMS, access control or SCADA are reached through flat networks or remote access.	Devices rebooting, setpoints changed, unknown remote sessions.	Segmentation, network access control, OT monitoring, IEC 62443.
Deepfakes & AI misuse	Fake voice or video of an executive requests urgent payments; staff paste sensitive data into AI tools.	An urgent "CEO" voice note; company data appearing in AI tools.	Verification procedures, AI usage policy, AI security and DLP controls.

Not sure which of these you are exposed to? **Get a free assessment →**

What each security layer does

No single product protects an organisation. These layers work together. We work across multiple brands and recommend on fit, not on a single vendor.

LAYER	WHAT IT DOES, SIMPLY	LEADING TECHNOLOGIES
Firewalls & network security	Guards the door between your networks and the internet.	Fortinet, Palo Alto Networks, Check Point, Cisco, Sophos, SonicWall, WatchGuard
Zero trust & SASE	Secure access for people working anywhere, replacing VPN.	Zscaler, Netskope, Cloudflare, Cato Networks, Fortinet, Cisco
Endpoint protection & XDR	Stops malware and ransomware on laptops and servers.	SentinelOne, CrowdStrike, Microsoft Defender, Trend Micro, Sophos, ESET, Kaspersky, Bitdefender
Email security	Blocks phishing, fraud and malicious attachments.	Microsoft Defender for Office 365, Proofpoint, Mimecast, Check Point Harmony
Identity, MFA & privileged access	Proves users are who they say; protects admin accounts.	Microsoft Entra ID, Okta, Cisco Duo, CyberArk, BeyondTrust, Delinea
SIEM, SOAR & SOC	Collects logs and alerts; a team watches 24/7.	Splunk, Microsoft Sentinel, Google Security Operations, IBM, FortiSIEM
Data protection & DLP	Finds sensitive data and stops it leaving.	Data Resolve inDefend, Microsoft Purview, Forcepoint, Varonis
Insider-threat monitoring	Spots risky behaviour and data theft by insiders.	Data Resolve inDefend, Microsoft Purview Insider Risk, Forcepoint
Cloud security	Checks cloud settings and protects workloads.	Microsoft Defender for Cloud, AWS security services, Wiz, Prisma Cloud
OT & building systems	Protects CCTV, BMS, access control and plant networks.	Claroty, Nozomi Networks, Cisco Cyber Vision, Fortinet OT
Network access control	Only approved users and devices may connect.	Cisco ISE, Aruba ClearPass, Forescout, FortiNAC
Vulnerability management	Finds weaknesses and tracks the fixes.	Tenable, Rapid7, Qualys, ManageEngine
Web & API security	Protects websites and apps from bots and attacks.	Akamai, Cloudflare, Imperva, F5
Backup & recovery	Copies attackers cannot delete, and tested restores.	Veeam, Rubrik, Commvault, Acronis
Awareness training	Turns staff into a line of defence.	KnowBe4, Proofpoint, Microsoft Attack Simulation
Incident response	Contains, investigates and recovers when an attack gets through.	Microsoft Defender XDR, CrowdStrike, SentinelOne

See all 27 layers on nice-venture.com/cybersecurity. Trademarks belong to their respective owners.

What's changing: today's security priorities

Threats move fast. These are the shifts every organisation should prepare for now.

AI-powered phishing & deepfakes

Flawless phishing in any language and fake executive voice or video. Answer: phishing-resistant MFA, payment verification rules, updated training.

Securing AI tools and agents

Staff use AI assistants and companies deploy AI agents. Answer: AI usage policy, data-leak controls, agent permissions, ISO/IEC 42001 governance.

Identity is the new perimeter

Most breaches start with a stolen login. Answer: passkeys and phishing-resistant MFA, identity threat detection (ITDR), privileged access.

Continuous exposure management

Annual tests are no longer enough. Answer: continuous attack-surface, vulnerability and configuration monitoring.

Data security posture

Sensitive data is scattered across cloud and SaaS. Answer: data discovery and classification, DLP, insider-threat monitoring.

Building and OT exposure

CCTV, BMS and SCADA are now connected. Answer: segmentation, NAC, OT monitoring and IEC 62443 by design.

Post-quantum readiness

Future quantum computers threaten today's encryption. Answer: a cryptography inventory and migration roadmap.

Stricter regulation and insurance

Privacy laws, sector rules, NIS2 and DORA in Europe, and insurers all demand proof of controls. Answer: mapped controls and evidence.

Want to know which of these matter most for you? **Talk to us →**

10 first steps for every organisation

These ten steps stop most of the attacks in section 2. Tick off what you already have.

1. Turn on multi-factor authentication for every account, starting with email and administrators.
2. Keep an up-to-date list of your devices, software, cloud accounts and important data.
3. Patch operating systems, firewalls, VPNs and key applications every month.
4. Replace basic antivirus with endpoint detection and response (EDR).
5. Back up important data with at least one offline or immutable copy — and test a restore.
6. Secure email with filtering and DMARC, and call back before changing any bank details.
7. Give people only the access they need; keep admin accounts separate from daily accounts.
8. Train staff and run phishing simulations at least twice a year.
9. Separate CCTV, BMS and IoT devices from your business network.
10. Write a one-page incident plan: who to call, what to disconnect, how to restore.

Want us to check these ten steps for you? **Book a free security assessment →**

When an attack gets through

No defence stops everything. What matters is how fast the damage is contained and how completely it is corrected.

If you think you are under attack: do not switch off or wipe affected machines — disconnect them from the network. Keep emails, logs and ransom notes. Change passwords from a clean device. If money was sent, call your bank immediately. Then WhatsApp us now or call +971 55 134 6136.

1. Prepare

Plan, contacts, playbooks, logging and tested backups — rehearsed before anything happens.

2. Detect & triage

Confirm the incident, judge its severity and preserve evidence.

3. Contain

Isolate devices, disable compromised accounts, block malicious traffic.

4. Investigate

Find how the attacker got in, what they accessed, and whether data left.

5. Eradicate & recover

Remove the attacker, close the entry point, restore clean systems.

6. Learn & harden

Report, fix the root cause, update controls and training.

Read more: Incident Response & Recovery

The standards worth knowing

NIST CSF 2.0

Six functions — Govern, Identify, Protect, Detect, Respond, Recover — used worldwide to structure security programmes.

ISO/IEC 27001

The international certifiable standard for an information security management system.

CIS Controls v8

A prioritised list of practical safeguards; an ideal starting point for smaller organisations.

IEC 62443

Security for industrial and building control systems — BMS, SCADA and OT.

PCI DSS v4.0

Required wherever payment cards are taken: retail, F&B, hospitality, e-commerce.

UAE IA, Dubai ISR, ADHICS

Security requirements for UAE government, Dubai government and Abu Dhabi healthcare.

UAE PDPL & GDPR

Laws protecting personal data — customers, staff, CCTV footage and marketing lists.

ISO/IEC 42001

A management system for the responsible and secure use of AI.

Regulations change; confirm current obligations with your legal or compliance adviser.

How to choose a cybersecurity partner

1. Do they start with an assessment of your risks, not a product?
2. Can they offer more than one brand, and explain why they recommend one?
3. Do they align the work to recognised standards such as NIST CSF, ISO 27001 or CIS Controls?
4. Will they document what they deploy and train your team at handover?
5. Can they secure building systems and OT, not only office IT?
6. Do they offer monitoring and a clear plan for the day an attack gets through?
7. Are licence renewals, support and escalation defined in writing?

Glossary

TERM	MEANING
EDR / XDR	Endpoint / extended detection and response
MDR	Managed detection and response — outsourced 24/7 monitoring and containment
MFA	Multi-factor authentication — a password plus a second proof
SOC	Security operations centre — the team that monitors and responds
SIEM	Central collection and analysis of security logs
SASE / ZTNA	Cloud-delivered network security / zero trust access replacing VPN
DLP	Data loss prevention
UEBA	User and entity behaviour analytics
WAF	Web application firewall
PAM	Privileged access management
NAC	Network access control
OT	Operational technology — systems that control physical processes
VAPT	Vulnerability assessment and penetration testing
RPO / RTO	How much data you can afford to lose / how fast you must recover
DMARC	Email record that stops criminals sending mail as your domain
Zero-day	A weakness exploited before a fix exists
vCISO	Virtual chief information security officer — part-time security leadership

Talk to us

NICE Venture designs, deploys and supports cybersecurity programmes aligned with NIST CSF, ISO 27001, CIS Controls and IEC 62443 — from essential protection to advanced defence, across a multi-vendor ecosystem.

Free security assessment
WhatsApp us to book

WhatsApp
+971 55 134 6136

Call
+971 55 134 6136

Email
sales@nice-venture.com

Request a proposal
nice-venture.com/request-a-proposal

Under attack now?
Urgent incident response

NICE Venture Information Technologies LLC · Al Khabeesi Building, Deira, Dubai, UAE · nice-venture.com

This guide is general information, not legal advice. © NICE Venture Information Technologies LLC.