ManageEngine

Endpoint Security Essentials

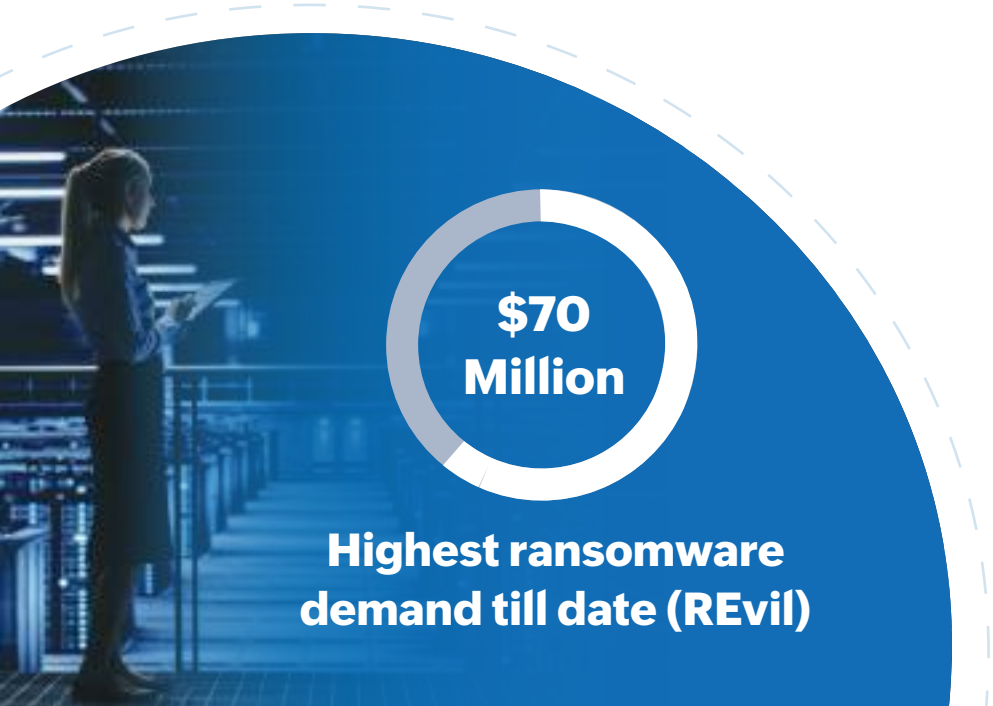
for the C-Suite

An executive's digital dilemma: With great tech comes greater risks

As our reliance on digital systems and technology increases exponentially, only cyberattacks have outpaced this massive surge—in terms of both scale and severity. Digital transformation is inevitable, but what surprises us the most is that it has been catalyzed by the pandemic. Two years after we've entered the new normal, thought leaders and the C-suite are still grappling with the next biggest hurdle in innovation—rising cyberthreats and the inability to plug security gaps in business.

Cyberthreats are an unnecessary byproduct of digital everything, hurting businesses worldwide. **The highest ransomware demand to date is $70 million in the REvil attack.**

While IT and cybersecurity professionals adapt to the new normal, thriving in it amid countless cyberthreats is a different game altogether. It's time for CTOs, CIOs, CISOs, and business executives to get to the core of the problem, communicate, and understand the key cybersecurity challenges in their organization. When it comes to dealing with incidents and cyberthreats, business leaders must be able to facilitate these concepts:



Cybersecurity facilitation framework

Identify

The first step in addressing an incident is to identify one. In this phase, timing plays a crucial role in determining the extent of damage that a cyberthreat can inflict on your organization.

Measure

Measuring allows you to size up the extent of damage, so that you can access the time and resources you'd need to prevent the attack from getting worse.

Communicate

Communication is key when your organization is ground zero for a cyberattack. Leaders must ensure transparency and free-flow of information so that different teams can gel together with the aim to remediate the threat at hand.

Remediate

Leaders must not shy away from getting to the crux of the problem, and should always seek to learn and infer with an open mind while enabling a hassle-free remediation process.

Evolve

Even if threats can be eliminated, no organization can claim that their approach to curb attacks is foolproof. The only way to move forward is to learn from previous incidents and grow stronger with experience on your side.

ManageEngine

Potential consequences faced by the C-suite due to lack of cyber-preparedness

Disruption of business services

The aim of any business is not to provide security (unless you're a security company) but to invest time and energy refining products or services—be it mass-produced life-saving pills, or building the next generation of fuel-efficient cars. The CISO needs to ensure that cyberthreats don't obstruct innovation and consume precious time that could otherwise be used productively.

Financial losses

Apart from loss of time and data, cyberattacks come with their own overhead costs in the form of ransom, or data breach recovery that sometimes cost an organization significantly.

Public distrust

Even if the organization manages to recuperate from a cyberattack financially, it often tarnishes the corporate image, and causes loss of trust and faith among your most loyal customers; this is challenging to mend.

Inability to keep up with regulatory shifts

Failure to respect and comply with international data privacy laws can lead to governments levying hefty fines. In extreme cases, it is even likely that organizations could be barred from doing business in a particular country.

Cyberattack report card

1. DAMAGE ANALYSIS

1885% increase

in ransomware attacks on government targets in 2021.

2. KEY FUTURE TREND

By 2024 IT analysts predict

a cyberattack will critically damage IT infrastructure prompting a member of the G20 to reciprocate with a declared physical attack.

3. STATE OF CYBERATTACKERS

About 100 attempts per minute

were detected attempting to exploit a vulnerability in the Apache Log4j, a widely used software library, after one week of its discovery.

4. THE SILVER LINING

33% projected rise

in employment of information security analysts from 2020 to 2030. The average growth rate for all occupations is 8%.

References

1. Fortune | Ransomware attacks surge in 2021
2. Gartner | Top Predictions for IT Organizations and Users in 2022 and Beyond
3. ZDNet | Log4j flaw attackers are making thousands of attempts
4. US Bureau of Labor Statistics | Occupational Outlook Handbook

ManageEngine

Rethinking the cybersecurity leadership

Cyberattacks are a force to be reckoned with. As we grow and evolve, we need to restrategize traditional cybersecurity viewpoints and redefine the role of the C-suite in mitigating these risks.

Traditional approach vs modern approach

It's vital for organizations today to move beyond traditional approaches, and proactively implement modern strategies that focus on cooperative problem solving. The C-suite needs to become actively involved and lead on security issues, not leaving sole responsibility to the IT security team. Four points that illustrate the difference between the traditional approach and the modern approach are showcased below.

Traditional approach

- End goal of cybersecurity is to have zero breaches.
- Dealing with cyberattacks is the security team's responsibility.
- Cybersecurity principles should be applied only to technical teams.
- Data privacy laws limit business scope and stagger growth.

Modern approach

- End goal of cybersecurity is to simplify and expedite the remediation process.
- Cyberattacks are a major business risk that needs imminent attention.
- Cybersecurity should be a core part of any major team and department.
- Complying with data privacy improves digital trust and boosts credibility.

Key questions that will enable executives to gain the edge in cybersecurity

Which of our assets are exposed?

Digitization and modernization might lead you to expand the number of your managed devices in your organization which, in turn, might lead to an enlarged attack surface. That shouldn't deter you from cutting down on the number of devices that help you accelerate business goals and gain a competitive edge. It's advisable to have an idea of how many of your assets have been exposed to the internet so that when you face an attack, you're well-prepared to gauge the extent of the threat and take remediation measures against the given threat.

What are we doing to shield these assets from external threats?

A detailed list of measures to shield your attack surface against threats includes a combination of security components, policies, and provisions that address your organization's risk management. This includes keeping tabs on all laptops, desktops, mobile devices, IoT devices, wearables, and various point-of-sale devices round the clock.

What is our security perimeter comprised of?

A layered security approach is essential to any cyber-preparedness strategy. Every protective layer that is deployed serves a particular purpose. These layers might include implementing firewalls, enabling Zero Trust, installing intrusion detection systems, deploying threat prevention systems, and enforcing multi-factor authentication.

Do we have a mechanism to receive alerts about threats and vulnerabilities?

A cyber protection policy is incomplete without a way to detect threats beforehand. Do you have systems to scan, detect, and measure vulnerabilities and threats? It's time to reassess your threat detection measures.

What is our incident response plan?

An incident response plan acts as a rule book for a cyber crisis and details the steps required to meet the business policy. Key components of an incident response plan include proactive measures, transparency, collaboration, the ability to rebound from the crisis, analyzing the learning outcomes, and continuously improving your cyber preparedness.

Where should I allocate my resources?

No matter how much budget you allocate to bringing in top-skilled personnel and getting the best security products, you can never ensure zero incidents. What you can ensure is that your enterprise is using resources judiciously. You also need to gauge your stance in specific scenarios. For example, if you're under a ransomware attack, do you pay the ransom? It is advisable to sit with the security team, understand the implications and devise strategies to get around these questions.

The cybersecurity trinity that executives need to leverage

People

Identify third-party collaborators and facilitators. Build a security team around skilled personnel. Provide end-user education and awareness programs. Communicate with stakeholders.

Technology

Adapt to future trends. Expose the extent of the attack surface. Implement layered security. Gain a competitive edge.

Business

Establish an incident response plan. Promote interoperability and collaboration. Develop a business continuity plan. Conduct boardroom planning and discussion meetings.

ManageEngine

About ManageEngine unified enpoint management and Security

ManageEngine UEMS develops unified endpoint management and security tools for teams that are looking to adopt change and innovate fearlessly. Our unified endpoint management (UEM) solution automates tasks, delivers insights, and provides a reliable way to ensure management and security of your workforce. From a single dashboard, you can secure your organization by minimizing risks without affecting your agility. You're enabled to work smarter, stay informed, and accelerate your operations without any obstacles.

Visit ManageEngine's UEM Page

Find us on Gartner peerinsights Capterra G2

sales@manageengine.com | +1-925-924-9500

Follow us on

ManageEngine