Notes:

- These are meant to be meaty, like mini-blogs.
- The outline for each email precedes the draft.

Cisco U. security landing page: https://learningnetwork.cisco.com/s/cisco-u-security

Cybersecurity

Email 1: Gen AI and hacking

- Highlight the increasing cybersecurity challenges in the digital era.
The Gen AI tools that make creating easier for everyone have also made it easy for ad hoc, amateur hackers to create destructive code.
  - Discuss the risks of having an unprepared IT team (legal issues created by breach of customer information, leak of trade secrets)
  - Preview classes to help.
CTA: Go to Cisco U. cybersecurity page

Audience: B2B decision-makers, IT team
Subject: Cisco U.: Gen AI makes work easier for all—including hackers
Preview: Only 9% of companies are ready—are you?

Main link: https://u.cisco.com/explore?technology=Security

Hi <name>,

All over the world, generative AI is helping democratize businesses—allowing smaller teams unprecedented access to sophisticated production tools. Great, right?

Gen AI makes attacks easier for hackers
But there's a dark side to this new equity. Generative AI is also giving non-tech-savvy hackers ready access to methods of mass disruption, making it simpler for amateur coders to create destructive code at a larger volume. Over the past 12 months, 75% of security professionals reported an increase in attacks, with most attributing this to use of generative AI.[1]

The scale and scope of these cyber-assaults are growing. In research earlier this year, Microsoft found that Chinese-backed, Russian, North Korean, and Iranian hackers are using generative AI as tools to invade sectors across the board, including energy, transportation/logistics, and even non-governmental organizations.[2]

<<Protect your company with Cisco U. cybersecurity training>>

Companies aren't keeping up with internal generative AI cybersecurity risks
The fast rate at which generative AI is being adopted also means that many companies aren't keeping up with risk management, with even their own developers accidentally creating security vulnerabilities.[3]

A recent survey by Riskonnect found that while 93% of companies surveyed well understood the threats imposed by greater adoption of AI by their own companies, only 9% actually have a plan[4] in place to manage it. Underprepared IT teams mean:

- Data privacy issues, including breaches of customer information and the ensuing legal fallout
- Leaking of trade secrets and other intellectual property risks
- Decisions being made on potentially inaccurate AI
- Employee misuse
- High IT team attrition[5]

Be proactive, not reactive
The answer, then, is for companies[6] to not just react to threats, but to fortify against AI-led cyberattacks before they happen. The best way to do this is by building an elite cybersecurity squad with education that addresses the fast-changing landscape of AI threats.

Cybersecurity training at Cisco U. not only provides your professionals with the gold standard in networking education and certification, Cisco U. also publishes new content every month to address emerging cybersecurity issues. Courses, Learning Paths, webinars, hands-on labs, and access to experts—all in one place.

<<Get Cisco U. cybersecurity training before attacks happen>>

Here's to better preparation through education,

The Cisco U. Crew

1, 5 https://www.securitymagazine.com/articles/99832-study-finds-increase-in-cybersecurity-attacks-fueled-by-generative-ai

2 https://www.itpro.com/security/state-backed-threat-actors-are-using-generative-ai-en-masse-to-wage-cyber-attacks-according-to-microsoft-and-openai

3 https://techcrunch.com/2022/12/28/code-generating-ai-can-introduce-security-vulnerabilities-study-finds/

4 https://riskonnect.com/content-library/new-generation-risk-report/?portfolioCats=90

6 https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

---

Email 2: Understanding the Top Cybersecurity Issues

- Detail the current top five cybersecurity issues with brief examples and business impacts
-Generative AI-driven attacks
-Ransomware as a service
https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/-Social engineering
-Third-party breaches
-Cloud vulnerabilities
- Stress the importance of awareness and training to mitigate these threats.
CTA: Go to Cisco U. cybersecurity page
NOTE: seems like a great blog post topic for a Cisco expert, if we don't have it yet

---

Audience: B2B decision makers/IT team

Subject: Cisco U.: The top 5 cybersecurity threats companies face
Preview: Experts predict new twists on dangers

Main link: https://u.cisco.com/explore?technology=Security
Link to specific tutorials.

Hi <name>,

Today's dynamic cybersecurity landscape means not just putting up safeguards and responding to threats as they happen but predicting the future and setting up barriers to protect your business before dangers manifest.

The Cisco 2024 Cybersecurity Index finds that most companies are underprepared and overconfident in their ability to respond to complex new cybersecurity threats. The cost? Most incidents trigger losses of at least $300,000, with 12% coming in at $1 million or higher.

<<Safeguard your company with Cisco U. cybersecurity training>>

Same threats, new twists

It's important, then, to understand how criminals are evolving their operations. Here are five of the most pressing cybersecurity concerns for businesses.

1. **Generative AI**

   It's often said that AI is the worst it'll ever be—meaning the quality's only going to get better. While that helps companies scale up their business efforts, it also means that threat actors can also scale up their attacks. Large language mode (LLM) tools allow hackers to easily identify and exploit vulnerable assets, then launch automated attacks.[1] Defending against threat actors who use generative AI requires a considered, novel approach that incorporates using your own gen AI as part of your cybersecurity plan.[2]

2. **Ransomware-as-a-Service (RaaS)**
   There's nothing new about ransomware, where an attacker, usually some group, infiltrates a networking system and takes it over, demanding payment in return for release. But now hackers employ RaaS, a middleman that launches attacks on their behalf for a small fee or percentage of the take. Groups are now adopting new harassment tactics and finding that data may be more valuable than simple payment. Companies must secure themselves not just against individual threat actors, but against a thriving black market seeking to exploit their intellectual property. [3]

3. **Social engineering**
   No human is perfect—which also makes them the perfect cybersecurity targets. A harried, multi-tasking worker accidentally clicks on a legitimate-looking email, only to unleash a cybersecurity nightmare. New, related schemes, like cryptojacking—where devices are secretly commandeered to mine cryptocurrency—are always popping up.

Employers train as well as they can, but there's no guarantee humans won't make errors, especially when criminals are always seeking new ways to exploit and infiltrate. Safeguards must be put into place before they're even a problem to be solved.[4]

4. **Third-party breaches**
   Companies may have tight cybersecurity, but when companies give third-party companies privileged network access, hackers can then attack that third-party instead to gain access to valuable data.

   The rise of the remote workforce and independent contractors also pose more opportunities for security lapses. Companies must find ways to preemptively secure their extended cloud with safeguards like dentity intelligence, analyzing each user's behavior and actions overall before granting access—something that 82% of companies are still in the early stages of enacting. [5]

5. **Cloud vulnerability**
   Almost everything to do with data has moved to the cloud, but the cloud's getting less secure, not more. Third-party providers usually manage the cloud, and since every company has different security standards, breaches and weak points can go unnoticed. The old approach of patching doesn't work.

   Companies should look to using newer networking approaches, such as Secure Access Service Edge (SASE), which mixes traditional network security functions with software-defined wide-area networking (SD-WAN) capabilities to provide secure and reliable cloud access. However, only 22% of companies currently use SASE, while most stick to the old—and less secure—ways.[6]

Mitigating cybersecurity threats begins with education

Creating networking infrastructure that withstands all these cybersecurity threats and more means you have to understand the current dangers and be able to predict what's coming next. One of the keys to building the right guardrails is investing in ongoing cybersecurity training with the pros at Cisco U.

With the right skills, your team can detect and protect against threats faster. Cybersecurity education with Cisco U. can help you meet your safety benchmarks by teaching your team:

- How to secure a hybrid cloud environment
- Enabling safe hybrid work with identity intelligence
- The best observability solutions so they can predict and prevent attacks
- The latest in modern network infrastructure security

Then, new content every month keeps you up-to-date on the latest cyberthreats and how to handle them.

Understand future threats with Cisco U. cybersecurity training

Yours in cybersecurity learning,

The Cisco U. Crew

1 https://www.zscaler.com/blogs/security-research/top-5-cyber-predictions-2024-ciso-perspective

2, 5, 6 https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

3 https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

4https://www.embroker.com/blog/top-cybersecurity-threats/

Email 3: Fortifying Against Phishing and Social Engineering

1. Intro: set the stage/problem

- Offer strategies for staff training against phishing.

- Network monitoring, secured networks, and training can help. (Cisco U)

CTA: Go to Cisco U. cybersecurity page

Source to pull from:

Social engineering remains one of the most dangerous hacking techniques employed by cybercriminals, largely because it relies on human error rather than technical vulnerabilities. This makes these attacks all the more dangerous—it's a lot easier to trick a human than it is to breach a security system. And it's clear that hackers know this: according to Verizon's Data Breach Investigations report, 85% of all data breaches involve human interaction.

In 2023, social engineering tactics were a key method for obtaining employee data and credentials. Over 75% of targeted cyberattacks start with an email. Phishing is one of the top causes of data breaches, followed by the use of stolen credentials and ransomware. Phishing and email impersonation continue to evolve to incorporate new trends, technologies and tactics. For example, cryptocurrency-related attacks rose nearly 200% between October 2020 and April 2021, and are likely to remain a prominent threat as Bitcoin and other blockchain-based currencies continue to grow in popularity and price.

https://www.embroker.com/blog/top-cybersecurity-threats/

https://www.infosecurity-magazine.com/news/94-firms-hit-phishing-attacks-2023/

Audience: B2B decision-makers, IT team

Subject: Cisco U.: Hackers know—humans aren't perfect.

Preview: Combat new social engineering schemes

Hi <name>,

It starts with a legit-looking email from someone you trust—perhaps a colleague. “Can you help me out real quick?” it says. Your colleague’s asking you to fill out a form of some kind, with a link.

You’re in a hurry. You have a lot of work today and you’re late for a meeting. It’s not so different from other interactions with this colleague. It doesn’t even occur to you that it’s not safe.

You click on the link.

<<Prevent social engineering schemes with Cisco U. cybersecurity training>>

Social engineering schemes are no longer restricted to poorly worded emails from fake-looking addresses. They’re getting more sophisticated and rely on the one thing that will always be true: humans are imperfect. And over 85% of targeted cyberattacks involve a human element.[1]

Cybersecurity training

You can train your employees so they better recognize fake emails and phishing tricks, but the honest truth is that no matter how well they’re educated, people are still going to make mistakes. This means that when the inevitable happens, your company must be prepared with a rock-solid cybersecurity plan.

No matter where you are with a cybersecurity roadmap, Cisco U. can help. Whether your team is just adopting a cybersecurity training plan or are already authorities, Cisco U. has the right plan. Your team can stay ahead of the cybersecurity curve by learning how to:

- Enable secure hybrid work with Cisco Identity Services Engine (ISE), threat detection with Cisco XDR, and more
- Create secure infrastructure and other industrial networking concepts
- Explore observability solutions that let them better understand upcoming threats
- Secure a hybrid cloud environment

Plus, Cisco U. adds new content every month, so there’s always something more to learn.

<insert content cards: tutorials: suggest:

ISE Posture https://u.cisco.com/tutorials/5425

XDR https://u.cisco.com/tutorials/4497

ISE policy https://u.cisco.com/tutorials/3011>

<Upgrade your cybersecurity readiness with Cisco U. training >

Cheers to better cybersecurity training,

The Cisco U. Crew

1 https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report

---

Email 4: Defending against ransomware

- In February 2024, small liberal arts college Willamette University held a Tech Day conference on the subject of cyberattacks, among other things. By that evening, the college found itself under a ransomware attack that invaded their technical infrastructure with encryption and took down their internet and phones, demanding payment. It took more than a week to restore service.

https://www.salemreporter.com/2024/02/29/willamette-university-recovering-from-cyberattack-that-followed-its-tech-day/

- Preventing such attacks by securing IT infrastructure

-Cisco U. cyber security and networking

CTA: Go to Cisco U. cybersecurity page

Audience: B2B decision-makers, IT team

Subject: Cisco U.: Ransomware attacks affect orgs of all sizes

Preview: How will you respond to a technical invasion?

Hi <name>

Ransomware attacks are usually only reported in national news if they hit a major company, but they don't just affect corporations. They also affect places like small businesses and colleges. Nobody is exempt.

In February 2024, liberal arts college Willamette University held a Tech Day conference on cyberattacks, among other things. Ironically, by that evening, the college found itself under a serious ransomware attack that invaded their technical infrastructure and took down their Internet and phones, freezing all campus communications. The college refused to pay the extortion demand. It took more than a week to restore service. [1]

<Prevent ransomware attacks with Cisco U. cybersecurity training>>

The five pillars of cybersecurity readiness

Preventing such attacks takes securing networking infrastructure in new ways that address evolving, multi-pronged cybersecurity threats. The first step is benchmarking whether your org has the five pillars of cybersecurity readiness[2] and assessing where you are in adopting them:

- Identity Intelligence
- Network Resilience
- Machine Trustworthiness
- Cloud Reinforcement
- Artificial Intelligence (AI) Fortification

In a survey of more than 8000 companies, Cisco found that most places are underprepared, falling into the Beginner or Formative categories. But with cybersecurity education from Cisco U., your company can step up its pillars faster, deploying solutions and polishing skills to avoid devastating financial impact and downtime.

Your team will deep-dive into topics like:

- How to enable secure hybrid work by using identity intelligence solutions
- Securing a hybrid, multi-cloud environment
- Learning about network observability and how to pinpoint and prevent security issues
- Exploring infrastructure security solutions

Your team members can learn at their own pace no matter where they are, using hands-on labs, courses, Learning Paths, self-assessments, videos, and more. Plus, new content is added every month. All they need is a browser.

<<Adopt the 5 pillars with Cisco U. cybersecurity training>>

Cheers to better cybersecurity training,

The Cisco U. Crew

1 https://www.salemreporter.com/2024/02/29/willamette-university-recovering-from-cyberattack-that-followed-its-tech-day/

2 https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

---

Email 5: Addressing Advanced Threats and Cloud Security

-Intro: Prepare for state-sponsored and advanced cyber threats.

Today there are more than 40 APT (Advanced Persistent Threat)hacking groups linked to foreign governments (Guardian article), linked to a hack of a Microsoft Exchange email server in 2021 and other American companies in order to steal trade secrets and affect elections.

- Discuss the need for continuous learning.

- Recommend cloud security training and proactive skill-building.

CTA: Go to Cisco U. cybersecurity page

Audience: B2B decision-makers, IT team

Subject: Cisco U.: Training for APTs and cloud security challenges

Preview: Hacking groups growing in scope and sectors

Hi <name>,

Advanced Persistent Threat (APT) sounds like something out of a spy movie, but it's not. It's a cybersecurity term referring to hacking groups linked to foreign governments. And these groups don't just want to hack government-related sectors—their targets include high-tech, healthcare, education, nonprofits, financial services, business services, media, entertainment, automotive, and engineering. Today there are more than 40 APT groups worldwide.[1]

In 2021, the UK accused APT 31, a group out of China, hacked a Microsoft Exchange email server, of compromising global accounts. The group used phishing with links that stole private information to gain access, sending more than 10,000 emails, and were even able to affect home routers and other personal devices.[2]

<<Understand global threats with Cisco U. cybersecurity training>>

Reinforce your cloud

Today, with many companies using third-party cloud services and managing remote employees, it's important to ensure that your cloud is reinforced with a novel approach, such as Secure Access Service Edge (SASE). SASE mixes traditional network security with software-defined wide-area networking (SD-WAN) capabilities and, when consistently applied and maintained across different cloud platforms, provides a better security experience. [3]

Help your company meet cybersecurity benchmarks with training from Cisco U. Your team will learn:

- How the Cisco Cloud Protection Suite reduces your attack surface and simplifies multi-cloud operations
- Infrastructure security solutions and industrial networking
- Observability solutions to help predict and prevent attacks before they happen

And with access to Cisco U., you'll get brand-new content every month addressing new developments in cybersecurity, with access to hands-on labs, courses, Learning Paths, and experts.

<<Secure your cloud with Cisco U. cybersecurity training>>

Yours in learning,

The Cisco U. Crew

[1] https://www.mandiant.com/resources/insights/apt-groups

[2]https://www.theguardian.com/technology/2024/mar/26/china-cyber-attack-uk-us-explained-hack-apt-31

3 https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

---

Email 6: Prioritizing Identity and Access Management

-Discuss poor IAM in the 2017 Deloitte breach. Deloitte, with $37 billion in revenue, provided cybersecurity advice to governments and financial institutions. Yet hackers breached the global email server via an unrestricted admin account only guarded by a single password.
- Discuss the pivotal role of IAM in current cybersecurity strategies.

-Offer insights on enhancing IAM systems.
- Encourage enrollment in Cisco U. classes for IAM proficiency.

https://www.cisco.com/c/en/us/products/security/identity-services-engine/what-is-identity-access-management.html

Audience: IT teams, B2B decision-makers

Subject: Cisco U: How a single password took down a major company

Preview: Strengthen your cybersecurity with Identity Intelligence

Hi <name>,

It's a horror story that cybersecurity folks still tell. In 2017,[1] Deloitte, a company with $37 billion in revenue, who provided cybersecurity advice to financial institutions and governments alike, was hacked, their global email server compromised. The cause? An unrestricted admin account only guarded by a single password.

It was all due to a hole in their identity access management (IAM) process— making sure that the right people and entities have access. But there's more to IAM than most people are aware of.

<<Learn about Identity Intelligence with Cisco U. cybersecurity training>>

Identity intelligence
Today, advanced cybersecurity teams use identity intelligence[2], which not only understands who is trying to get network access, but the context of that access. Identity Intelligence analyzes the user's behavior and detects patterns and anomalies so it can identify potential breaches, such as the one that happened at Deloitte.

Identity Intelligence is a newer cybersecurity tool, but it's considered a pillar of cybersecurity preparedness. Cisco U. can help your team become an elite cybersecurity squad with education on:

- Securing a hybrid cloud environment
- Enabling hybrid work with identity intelligence
- Implementing modern network security
- Turning security insights into action with observability solutions

Team members can access content whenever they want, choosing from hands-on labs, courses, tutorials, self-assessments, and more, creating a personalized experience that still gets them upskilled fast. Plus, new content arrives every month, so the learning never gets stale.

<<Get the pillars of cybersecurity with Cisco U. training>>

Here's to the best in cybersecurity education,

The Cisco U. Crew

1 https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

2 https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

Email 7: Conclusion Email: Recap and Resources

-

- Summarize the key takeaways from the series, explaining how new threats are always emerging

- Provide additional resources and training opportunities.
- Encourage making cybersecurity skill development a continuous priority.
- Invite feedback and further inquiries about cybersecurity training.

Audience: B2B decision-makers, IT team

Subject: Protect your company with cybersecurity training
Preview: Give your team the right skills

Hi <<name>>,
With so many technological advances going on all the time, it's hard for most companies to prioritize and keep on top of cybersecurity threats. Yet it should be at the top of the list. More than half of companies that had a cybersecurity incident in 2023 said it cost their organization at least US $300,000, while 12% reported it cost US $1 million or more.[1] Add reputational risk, and the price climbs.

<<See how Cisco U. cybersecurity training can help you save on operational costs>>

Emergent cybersecurity threats
Cybersecurity threats that companies need to consider include:

- Generative AI that allows amateur threat actors to create destructive code
- Advanced Persistent Threat (APT) hacker groups, funded by governments, that attack across industries and take advantage of lax cloud security
- Phishing that uses new tactics to trick overtired humans and infiltrate personal devices
- Ransomware as a Service that provides bad actors with full-service hacking packages via the dark web

Coming up with a comprehensive cybersecurity plan is important. And one of the first steps in enacting a full cybersecurity plan is making sure your team is educated in all aspects of cybersecurity.

Cisco U. has cybersecurity training to help your company achieve its cybersecurity benchmarks. Your team will learn how to:

- Reduce your attack surface and secure your hybrid, multi-cloud operation as it scales
- Secure and enable hybrid work with identity intelligence
- Monitor data for performance and security with Cisco ThousandEyes and App Dynamics, and be able to predict problems instead of react
- Implement the latest in infrastructure security solutions

Cisco U. also gives your team access to ongoing education, with new monthly content that evolves to meet your emerging needs.

<<Achieve your cybersecurity benchmarks with Cisco U.>>

Cheers to cybersecurity training that protects,

The Cisco U. Crew

ttps://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf