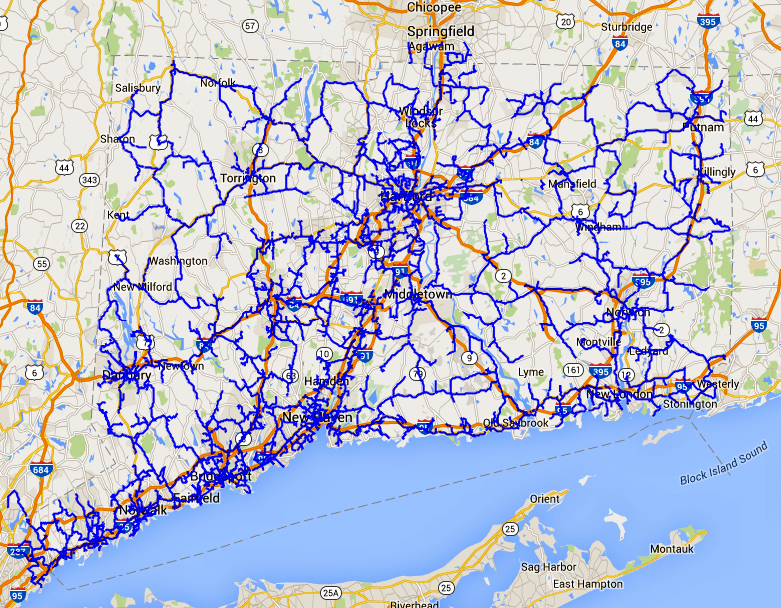
**Connecticut’s Defenses from Cybercrime Threats**

***Critical Assets Security and Risk Prevention***

**October 2018**

**Bill Vallee, Broadband Policy Coordinator**

**Office of Consumer Counsel, State Broadband Office**



Connecticut Education Network (CEN)

is part of the State's secure "Nutmeg Network"

|  |  |
| --- | --- |
|  |  |

Petya targeted drives, not files.  After 7 days the decryption key price doubles.

**Connecticut’s Defenses from Cybercrime Threats**

***Critical Assets Security and Risk Prevention***

**October 2018**

**Bill Vallee, Broadband Policy Coordinator**

**Office of Consumer Counsel, State Broadband Office**

Contents

[Introduction - National Cyber Security Awareness Month (NCSAM) 3](#_Toc526859014)

[Municipalities are vulnerable to attack 4](#_Toc526859015)

[Connecticut businesses are vulnerable 6](#_Toc526859016)

[Connecticut Business & Industry Association 7](#_Toc526859017)

[The Greater Hartford (Connecticut) Chapter of SCORE 7](#_Toc526859018)

[The State of Connecticut’s Cybersecurity Strategies and Plans 9](#_Toc526859019)

[2018 Cybersecurity Action Plan 9](#_Toc526859020)

[2017 Cybersecurity Study Pursuant to Special Act 15-13 10](#_Toc526859021)

[2017 Connecticut's Cybersecurity Strategy 11](#_Toc526859022)

[Connecticut Education Network (CEN) 12](#_Toc526859023)

[2014 Cybersecurity and Connecticut’s Public Utilities Report 13](#_Toc526859024)

[2013 Comprehensive Energy Strategy for Connecticut 14](#_Toc526859025)

[Workforce Development for Cybersecurity talent gaps 14](#_Toc526859026)

[Connecticut Cybersecurity Resources 16](#_Toc526859027)

[Cyber Security Meetups & Communities in Connecticut 16](#_Toc526859028)

[Resources in Case of an Attack 18](#_Toc526859029)

S:\SHAREDAT\Broadband\Cybersecurity\2018-1009 Cybersecurity in Connecticut BV white paper.docx

# Introduction - National Cyber Security Awareness Month (NCSAM)

[National Cyber Security Awareness Month (NCSAM)](https://www.dhs.gov/national-cyber-security-awareness-month) is [observed every October](https://portal.ct.gov/-/media/DAS/BEST/Security-Services/2018-Cyber-Security-Awareness-Month.pdf?la=en), and 2018 marks the 15th year of National Cyber Security Awareness Month. NCSAM was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online. Since its inception under leadership from the [U.S. Department of Homeland Security](https://www.dhs.gov/) and the [National Cyber Security Alliance (NCSA)](https://staysafeonline.org/ncsam/https:/staysafeonline.org/ncsam/about-ncsam/), comprehension of the importance of yber Security Awareness has grown exponentially, reaching consumers, businesses of all sizes, educational institutions and community anchor institutions across the nation.

[A 2017 strategic plan](#CyberStraty) developed by Governor Malloy and many state agencies and officials (detailed below), discovered that about 2 billion external connection attempts by cyber hackers to tap into the 3.5 million agency records relating to residents are blocked per month by state perimeter security measures.  In spite of these successful defensive efforts, the report said approximately 66 state and local systems are infected or compromised each month.

[Jim Hunt, an Eversource senior vice president for regulatory affairs, said](https://www.ctpost.com/local/article/Connecticut-s-defenses-deflect-cyber-attacks-13239189.php) the electric company fights off over 300 million cyberattacks a year from hackers seeking to disrupt the system or obtain customer information. ([bcummings@ctpost.com](mailto:bcummings@ctpost.com)) "These threats are real," Hunt said. "We estimate we get a million knocks on the door from threats every day." Hunt said Eversource and the state’s other utilities are addressing the threat even as hacking technology evolves and improves.

Art House, the state’s first [Chief Cyber Security Risk Officer](https://ctmirror.org/2016/10/12/arthur-house-to-leave-pura-oversee-cybersecurity-planning/), has noted that [a successful attack on the state’s water distribution system](https://www.ctpost.com/local/article/Connecticut-s-defenses-deflect-cyber-attacks-13239189.php) would be perhaps the most devastating of public utility hacks since, while electric power seems the most disruptive, in fact humans cannot live longer than 72 hours without water.

Noting the efforts of the state to combat cyberattacks over the 5 years or more, Elin Swanson Katz and Jack Betkoski are hosting an all-day [***Utility Infrastructure Security Conference***](https://www.eventbrite.com/e/utility-infrastructure-security-conference-tickets-48734533301)on October 15, 2018, (7am-5pm) in conjunction with [Upward Hartford](http://www.upwardhartford.com/contact-us/), a 34,000 square feet co-working space in the Hartford, Connecticut [Stilts Building](http://www.upwardhartford.com/contact-us/), an event uniquely designed to support startups, change-makers, and entrepreneurs where ideas and projects can be launched, and connections can be made. This cybersecurity event is for utility executives, state utility commissioners, and state utility consumer advocates, and focuses on utility cyber security, drones, and infrastructure technology.

[OCC Consumer Counsel Elin Swanson Katz](https://www.ct.gov/occ/site/default.asp) is the president of the [National Association of Utility Consumer Advocates (NASUCA)](http://nasuca.org/), composed of agencies designated by state law to act as independent ratepayer advocates while its sister association is the [National Association of Regulatory Utility Commissioners (NARUC)](https://www.naruc.org/), a non-profit organization dedicated to representing the State public service utility regulatory commissions. In a timely coincidence, NARUC’s president is longtime Public Utilities Regulatory Authority (PURA) vice chairman and commissioner, [Jack Betkoski](https://www.ct.gov/pura/cwp/view.asp?a=3351&Q=455206#JWB).

# Municipalities are vulnerable to attack

There are [substantial cybersecurity risks for Connecticut’s 169 municipalities](https://www.jdsupra.com/legalnews/municipalities-under-connecticut-s-new-73858/) as cyberattack hacks are becoming far more common, as a 2016 [survey](https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf) of US [local municipality chief information officers](https://www.cio.com/article/3184618/government-use-of-it/county-and-municipal-cybersecurity-part-1.html) discovered (2016 Muni CIO survey). [As one report noted](https://www.nsiserv.com/blog/cybersecurity-risks-for-ct-municipalities-how-towns-fight-back), one-third of such digital invasions are ransomware attacks. The survey determined that 1/4th of towns were subject to some kind of hack attack, as often as once an hour, at the least.

Recognizing that cyber security is the number one threat for state and local governments, as part of its municipal training programs, the [Connecticut Conference of Municipalities (CCM)](https://www.ccm-ct.org/) held a [May 2018 Cyber Security Awareness Workshop](https://www.ccm-ct.org/Cyber-Security-05-08-18) to prepare town leadership for the cybersecurity challenges that local governments are facing across the state. The workshop focused on the vulnerabilities and threats to business operations to increase make employee awareness of their responsibilities and accountabilities when using a computer on a local government network. Further, CCM provides [Cybersecurity Advisory Bulletins](https://www.ccm-ct.org/cybersecurity-bulletins) designed for technology infrastructure owners and administrators to make them aware of threats or activity with the potential to impact their computer networks and IT infrastructure.

Thus, it has become obvious to experts that local and [state](https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/) governments must take greatly enhanced steps to ensure they are defended against such attacks, escalating the priority for funding and attention to this issue as they do for police and fire security. While many municipalities and states incorrectly regard [100% of hacks as being entirely outside threats](https://www.cio.com/article/3184618/government-use-of-it/county-and-municipal-cybersecurity-part-1.html), it is estimated that nearly all successful hacks [result from an internal mistake](https://www.cio.com/article/3184618/government-use-of-it/county-and-municipal-cybersecurity-part-1.html#_edn8), and 60% of breaches are a [result of internal attacks](https://www.cio.com/article/3184618/government-use-of-it/county-and-municipal-cybersecurity-part-1.html#_edn9). Thus, education and sharper focus will lead to more effective and less expensive defenses, if properly implemented.

The potential damages from a cyberattack on a municipality cannot be underestimated. For instance, [Wired analyzed the Atlanta ransomware hack of March 2018](https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/) in which it was reported that the city spent $2.6 million (later revised up to $10 million) to recover from a $52,000 ransomware holdup by attackers which [The New York Times described](https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html) as being “one of the most sustained and consequential cyberattacks ever mounted against a major American city.” Using the SamSam malware, the hackers were able to disrupt or destroy nearly half the city’s local government departments, including the police records system, infrastructure maintenance requests, revenue collection, and the judicial system. Not surprisingly, the invaders were never discovered, let alone apprehended, though this attack was far worse than in Dallas the year before when attackers [set off tornado sirens](https://www.dallasnews.com/news/dallas/2017/04/08/emergency-sirens-blare-across-dallas-county-despite-clear-weather) after midnight.

Of course, Atlanta could have better spent those millions of dollars, especially if the money had been spent to bolster defenses and reaction processes against cyberattacks. Wired reported in August 2018 on [The Untold Story of NotPetya, the Most Devastating Cyberattack in History](https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/) a Russian ransomware attack intended to disrupt government operations in Ukraine, but which cascaded across the world and destroyed entire networks with tens of thousands of computers with a cost of over $100 billion (Atlanta’s $10 million loss was thus a mere tenth of a percent of NotPetya’s price), stripping the record set by the roughly $6 billion cost of the [WannaCry](https://www.wired.com/tag/wannacry/) worm attack of May 2017.

The costs of remediation in such attacks include the rebuilding of the networks and equipment, plus lost business and reimbursement of customer losses and costs. Repercussions for businesses or their customers could include:

* Financial loss from banking and credit card data as well as equipment and other capital costs due to system and security enhancements.
* Loss of one’s identity, which can also require significant cost and effort to reclaim. Damaged reputation and loss of consumer confidence.
* Opportunity cost of time lost to recovery efforts.
* Decline in morale, both for business owners and employees.
* Potentially going out of business, in extreme cases.

As the NotPetya attack on Ukraine demonstrated, cybersecurity attacks can escape their intended victims and inflict “collateral damage” on municipalities, states, residents and businesses to a devastating degree, and thus defenses must be like vaccinations: everyone must be inoculated to prevent the spread of the disease and misfortune.

# Connecticut businesses are vulnerable

All [businesses are the juiciest targets for hackers](http://www.abcactionnews.com/news/security-expert-getting-hacked-a-matter-of-when-not-if) since they often hold extremely personal information and data for thousands or millions of consumers. Accordingly, it is essential that [businesses take and continually update actions](https://www.nsiserv.com/business-it-grader?__hssc=263450515.1.1539018472043&__hstc=263450515.9e034e193be94c5281630591679ae79f.1538662795893.1538662795893.1539018472043.2&__hsfp=1629656054&hsCtaTracking=174b30d8-c178-45b9-bcdd-1e2fcdf2c80a%7Cf42cd9e4-e004-4530-b379-55960f0493fb) to address [data security](https://www.nsiserv.com/network-support-computer-services-CT/bid/72797/Avoid-Heartbreak-Invest-in-Solid-Data-Backup-Solutions), particularly the big business of hacking personal information, in order to secure customers’ personal data, such as social security and credit card numbers.

Consumers are obvious hacker targets and to help protect them, the Connecticut state legislature has enacted a general privacy law, C.G.S. Chapter 743dd, [Protection of Social Security Numbers and Personal Information](https://www.cga.ct.gov/2017/pub/chap_743dd.htm) and a [2015 law](https://www.cga.ct.gov/2015/ACT/PA/2015PA-00142-R00SB-00949-PA.htm) (*An Act Improving Data Security And Agency Effectiveness)*that requires businesses to provide identity theft protection services if a [customer’s personal data is stolen](https://www.jacksonlewis.com/resources-publication/new-connecticut-law-requires-businesses-offer-identity-theft-protection-services-after-data-breach). The loss of identity information and data can allow thieves to loot bank accounts, make fraudulent credit purchases, steal income, and sell private information on the dark web. The exposure of private data can inflict dreadful personal damage to the victim, with negative effects on personal relationships, jobs, health, and safety. Employees of businesses charged with safeguarding such information can lose their jobs, be subject to civil judicial actions, or even fined or jailed under criminal laws.

Businesses themselves at the least will lose the trust of their customers and, as noted above in the dangers and costs presented by cyberattacks on municipalities, adding in the cost of disgruntled customers leaving the firm, providing theft protection services and customer notification, a data breach can be [extremely expensive for businesses](https://www.nsiserv.com/10-mistakes-most-connecticut-small-business-owners-make) of all sizes, but of course small businesses may suffer the worst since their financial cushion may be inadequate for the [remediation costs](http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/) of a cyber robbery or network destruction.

[Healthcare service providers](https://www.nsiserv.com/network-support-computer-services-ct/4-lessons-learned-from-recent-healthcare-data-breaches) are subject to extensive state and [federal rules](https://searchhealthit.techtarget.com/definition/HITECH-Act) and regulations regarding the highly sensitive information they hold about patients. For instance, [credit card data](http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5) may be purchased on the internet for a few dollars, but electronic medical and bank account records (containing very valuable identification numbers and sensitive healthcare information) may sell for far more.

## Connecticut Business & Industry Association

The [Connecticut Business & Industry Association](https://www.cbia.com/) conducted its first-ever [Cybersecurity Survey of Connecticut Businesses](https://www.cbia.com/resources/cybersecurity/cybersecurity-whitepapers/cybersecurity-survey-businesses/) to alert businesses across the state of the dangers of cyberattacks and to get a sense of their level of preparedness. In the 2018 [CBIA Cybersecurity Survey](https://www.cbia.com/wp-content/uploads/2018/03/Cybersecurity_18.pdf), CBIA detailed how companies are preparing for addressing prevention, minimizing damage, raising threat awareness among employees, and developing effective responses to attacks. [CBIA has developed programs and educational materials](https://www.cbia.com/resources/cybersecurity/cybersecurity-webinars/one-click-away-cyberattack/) for small to midsize businesses which are some of the most vulnerable targets for cyberattacks, including [vendor security strategies](https://www.cbia.com/wp-content/uploads/2017/09/ATT-Security-CBIA-Presentation-PDF.pdf) that can be incorporated into company plans.

Similarly to the [Muni CIO Survey](#MuniCIOsurvey), CBIA determined that about 1/4th of the state’s businesses suffered data breaches or cyberattacks in the last two years, with only 18% having an annual budget dedicated to cybersecurity. Nearly half the companies provide cybersecurity training to employees, but only a half of those make training mandatory. Also like the NotPetya attack on Ukraine, while most CT companies have a disaster recovery or business continuity plan, only 1/5th have an incident response plan in place for vendors, customers, and subsidiary operations, so collateral damage could be a very serious loss for attacked companies.

## The Greater Hartford (Connecticut) Chapter of SCORE

Founded in 1964 as a charter member of the National SCORE Association, [The Greater Hartford (Connecticut) Chapter of SCORE](https://greaterhartford.score.org/resource/how-protect-your-small-business-cyber-attack) has been highly active in alerting small and innovative businesses to the dangers of cyberattacks as part of its mission to match the experience of seasoned business owners and managers to the problems and challenges confronting existing and prospective small business owners. The [Greater Hartford SCORE is located](https://greaterhartford.score.org/contact-us-34) at 280 Trumbull Street in Hartford and is a nonprofit resource partner with the U.S. Small Business Administration (SBA).

[Hartford SCORE is a source](https://greaterhartford.score.org/search/site/cybersecurity) of free and confidential small business advice for entrepreneurs and small businesses, offering free business mentoring and low- or no-cost workshops:

* [What Your Startup Needs to Know about Cybersecurity](https://greaterhartford.score.org/resource/what-your-startup-needs-know-about-cybersecurity)
* <https://www.nationwide.com/about-us/083115-small-biz-survey.jsp>
* <https://www.staysafeonline.org/ncsam/resources/3-reasons-hackers-love-your-small-business-infographic>
* [Cyberattacks Cost Small Businesses More Than Money](https://greaterhartford.score.org/blog/cyberattacks-cost-small-businesses-more-money) about the rise of [ransomware](https://greaterhartford.score.org/blog/dont-let-your-business-be-held-ransomware), in which hackers hold your business data for ransom, but that's not the only threat to your small businesses’ cybersecurity.
* [How to Protect Your Small Business from a Cyberattack](https://greaterhartford.score.org/resource/how-protect-your-small-business-cyber-attack) reporting that about 50% of small businesses have experienced a cyberattack and more than 70% of attacks target small businesses. Also see the accompanying [Guide](https://s3.amazonaws.com/mentoring.redesign/s3fs-public/Cyber-Security-Eguide-Paychex-SCORE.pdf), which notes that small businesses are a particularly vulnerable target because they possess richer data assets than average consumers, but don’t have the protection of larger businesses.
* [How to Protect Your Small Business from a Cyberattack](https://greaterhartford.score.org/resource/how-protect-your-small-business-cyber-attack), Guide: As many as 60% of small and medium size businesses that experience a data breach go out of business after 6 months. A 2015 Small Business Owner Study, conducted by Harris Poll, shows: 75 percent of small businesses do not have a disaster plan in place. 52 percent say it would take at least three months to recover from a disaster.
* [Small Business Owners Optimistic—But Facing Risks](https://www.score.org/blog/small-business-owners-optimistic-facing-risks) provides a summary of the ninth edition of the [Hiscox DNA of an Entrepreneur Report](https://www.hiscox.com/documents/DNA-of-an-Entrepreneur-Report-2017.pdf) which has begun to cover the mounting threat of cyberattacks on businesses, basing its findings on responses from more than 4,000 owners and senior executives in businesses with fewer than 50 employees across Europe (France, Germany, The Netherlands, Spain and the United Kingdom) and the USA.
* One in eight firms (13%) has suffered a cyberattack, up from 11% the previous year. In the US and Germany, it is around one in six (16% and 15% respectively). Among those who have suffered a cyberattack, the proportion saying it resulted in a serious loss has nearly doubled this year – from 26% to 48% (p10).
* In all, around one in eight firms (13%) say they have suffered a cyberattack, up from 11% the previous year. The figures are highest in the US (16%) and Germany (15%). Among those who have suffered an attack, the proportion saying it resulted in a serious loss has nearly doubled this year – from 26% to 48%.
* While the threat of a cyberattack is recognized by an increasing number of respondents, relatively few firms have embraced insurance in this area. Overall, the number with cyber and data cover is up from 8% to 9% this year. Some 10% of US small businesses also say they are covered. Financial services and TMT firms are most likely to carry cyber and data insurance – 15% of them in each case.
* However, despite the relatively low proportion of firms that have cover in this area, there has been a dramatic rise in the number that say they have been able to make an insurance claim in respect of a cyberattack. Overall, among firms that have suffered an attack, 42% say they were able to claim – up from just 16% a year ago, with US cyberattack victims being able to claim on an insurance policy rising from only 15% to 59% between 2016 to 2017.

# The State of Connecticut’s Cybersecurity Strategies and Plans

## [2018 Cybersecurity Action Plan](https://portal.ct.gov/-/media/DAS/BEST/Security-Services/CT-Cybersecurity-Action-Plan-Final.pdf?la=en)

[Connecticut issued](http://www.hartfordbusiness.com/article/20180504/NEWS01/180509951/ct-launches-cybersecurity-action-plan) a 41-page [Cybersecurity Action Plan](https://portal.ct.gov/-/media/Office-of-the-Governor/Press-Room/20180503-CT-Cybersecurity-Action-Plan.pdf?la=en) (2018 Cybersecurity Action Plan) on May 3, 2018, which evaluated cyberattack challenges state government, municipal government, private business, higher education and law enforcement face in the Digital Economy. [By objectively reviewing facts and data](http://www.wnpr.org/post/malloy-launches-plan-enhance-connecticuts-cybersecurity), the 2018 Cybersecurity Action Plan was [effectively a “call to arms”](https://statescoop.com/in-a-call-to-arms-connecticut-publishes-cybersecurity-action-plan) for increased actions by all interested parties to protect the digital assets from the threats and potential damage brought by hackers operating in the cyber world.

The 2018 Cybersecurity Action Plan coincidentally followed a[February cybersecurity attack](http://www.hartfordbusiness.com/article/20180226/NEWS01/180229928) that infected 160 computers across 11 different agencies that state government action successfully defended and restored. [Mark Raymond, the Connecticut CIO stated](https://gcn.com/articles/2018/02/26/connecticut-wannacry.aspx) that the [WannaCry ransomware virus](https://gcn.com/blogs/cybereye/2017/05/wannacry-lessons.aspx) was the perpetrator in this attack, but he noted that the state’s security monitoring system alerted officials and IT staff worked through the weekend to contain the malware and secure all affected computers. Raymond pointed out that regular patches and antivirus software on the state’s more than 30,000 devices prevented a far worse result. A month later, another [ransomware attack](http://www.courant.com/business/hc-biz-state-cybersecurity-20180503-story.html) crippled hundreds of servers operated by the state courts in March.

The message is clear that malware viruses target undefended networks by employing various attack strategies and security backdoors. Thus, the 2018 Cybersecurity Action Plan properly sets goals for a statewide cybersecurity response and recovery strategy, including state agency and business community recovery plans for continuity of operations through annual exercises, among many other recommendations. It is obvious that the best defense against such attacks is a good offense: thus it is a better policy to regularly maintain security software updates and back up data than waiting to merely clean up after an attack.

Like many other suggestions over the last few years, the 2018 Cybersecurity Action Plan nods to voluntary action on the part of the general business community and the regulated public service utilities, but the Plan also states that since cybersecurity has become a compelling public issue of grave seriousness, that the dangers presented may require legislation and regulation through the political process. The Plan notes that financial service companies now face cybersecurity requirements in New York State. Businesses such as hospitals are already subject to confidentiality rules concerning health records, national security data requirements impact the many defense contractors operating in Connecticut, the state’s insurance companies handle many types of digital records, and public utilities provide critical services subject to many regulations.

## 2017 Cybersecurity Study Pursuant to Special Act 15-13

[Special Act 15-13 "An Act Concerning Cybersecurity"](https://www.cga.ct.gov/2015/ACT/SA/2015SA-00013-R00HB-06317-SA.htm) directed the [Department of Administrative Services (DAS)](https://portal.ct.gov/das) in consultation with the [Department of Emergency Services and Public Protection (DESPP)](https://www.ct.gov/despp/site/default.asp) to conduct [a study to identify cybersecurity issues facing the state](http://das.ct.gov/images/1090/2017%20DASCybersecurityReport%20SA%2015-13.pdf) (January 1, 2017) including recommendations and coordination efforts amongst impacted stakeholders--government, law enforcement, to improve cybersecurity preparedness in the State of Connecticut.

## [2017 Connecticut's Cybersecurity Strategy](https://portal.ct.gov/-/media/Office-of-the-Governor/Connecticut-Cybersecurity-Resource-Page/Connecticut-Cyber-Security-Strategy.pdf?la=en)

The [Connecticut Cybersecurity Strategy](https://www.cbia.com/wp-content/uploads/2017/09/Connecticut-Cybersecurity-Strategy.pdf) (­2017 Cybersecurity Strategy) was prepared by strategic group led by [Mark Raymond, the Chief Information Officer in Connecticut](http://www.hartfordbusiness.com/article/20110519/NEWS01/305199987/ct-hires-mark-raymond-as-cio) and [Chief Cybersecurity Risk Office Arthur House](#ArtHouse), was [issued by Governor Malloy](https://portal.ct.gov/DAS/Press-Room/Press-Releases/2017/Gov-Malloy-Releases-Cybersecurity-Strategy-for-Connecticut) on July 10, 2017. The 2017 ­Cybersecurity Strategy sets forth [a holistic approach](http://www.govtech.com/policy/Connecticuts-New-Cybersecurity-Strategy-Takes-Holistic-Approach.html) tapping into five key sectors state government, local government, business, higher education, and law enforcement and security to preparing defenses. This new strategy focuses on seven foundational principles the form an action plan which can be adapted to fir all public or private entities:

* executive leadership and awareness,
* literacy,
* preparation,
* response,
* recovery,
* communication and
* verification

[At the heart of the plan is the need for leadership](https://gcn.com/articles/2017/07/13/connecticut-cyber-strategy.aspx), thus the strategy’s primary audience is Connecticut’s leaders of five sectors of community interests across the state: the General Assembly, Judiciary, municipal governments, businesses, civic organizations, higher education institutions and law enforcement units.

The report concluded the first review of utility cybersecurity probes under a new voluntary program finalized by the Public Utilities Regulatory Authority last year. The report calls for greater cooperation among [all interested parties](file:///\\deep\public\NewBritainShared\OCC\SHAREDAT\Broadband\Cybersecurity\FBI-led%20cyber%20security%20unit%20forms%20as%20online%20crime%20spikes%20in%20Connecticut%20%20Oct%2024,%202017) in the effort to create cyberattack defenses and the state is called upon to encourage more municipalities to join, either directly or through trade association representation, Connecticut’s Cybersecurity Committee, a venue for state and town representatives to discuss threats, priority concerns and best practices. The [municipalities are called upon to join and utilize](https://www.jdsupra.com/legalnews/municipalities-under-connecticut-s-new-73858/) the shared internet protections provided by the Connecticut Education Network (CEN), and as of today, nearly all of the state’s school districts, libraries and municipalities are now members of the CEN.

## [Connecticut Education Network (CEN)](https://www.ct.gov/cen/site/default.asp)

The Connecticut Education Network (CEN) is part of the State's secure "Nutmeg Network", whose purpose is to deliver reliable, high-speed internet access, data transport, and value added services to its members throughout Connecticut. Established in 2000 to integrate high speed fiber optics networks into institutions of education statewide, CEN is governed by the [Commission for Education Technology](https://www.ct.gov/ctedtech/site/default.asp) (CET). [CEN’sfirewall service](https://www.ct.gov/cen/cwp/view.asp?a=4306&q=511308) controls the traffic that goes in and out of its network customers to protect them from hacking by offering Unified Threat Management covering Network Intrusion Prevention, Gateway Antivirus, Gateway Antispam, and Data Leak Prevention (DLP).

As the most recent of the members of the CEN (educational institutions and libraries have been members for many years), it remains a key component of the state’s cybersecurity plans that municipalities pursue the "initial strategic objectives" of the ­2017 Cybersecurity Strategy, including:

1. Increase civic awareness of cyber dangers; identify "prevention measures"; investigate cyber breaches; and prosecute cybercrimes.
2. Joint efforts to make cyber defense "a shared learning experience" and cost-sharing.
3. Embrace collaboration with the State Department of Administrative Services and its Bureau of Enterprise Systems and Technology, which provides security protocols for the executive branch of State government.
4. Assess municipal cyber security efforts in other states.

[**2016** **Connecticut Public Utilities Cybersecurity Action Plan**](https://www.ct.gov/pura/lib/pura/electric/cyber_report_April_6_2016.pdfhttps:/www.ct.gov/pura/lib/pura/electric/cyber_report_April_6_2016.pdf)

The 2016 PURA Cybersecurity Action Plan was issued by the PURA on April 6, 2016 in Docket No. 14-05-12 *PURA Cybersecurity Compliance Standards and Oversight Procedures* and opened with the statement:

Public utilities in Connecticut and throughout the United States face the credible danger of cyber penetration, compromise and disruption. National deterrence and remediation must include action at the state level including partnership among public utilities, their regulators and emergency response managers.

2016 PURA Cybersecurity Action Plan, at 1.

In this Report, PURA sought voluntary collaboration with Connecticut’s public utilities to review the adequacy of cyber defenses, reaching concurrence on standards and holding annual meetings with government participants. PURA noted that this collaboration had produced new solutions for enhanced cybersecurity, public understanding of such collaboration and rudimentary plans with the electricity, natural gas and water sectors.

PURA examined the effects of the [Russian cyberattack on Ukraine](#Ukraine) (discussed above in Municipalities) in great detail, concluding that:

The incident is a concrete instance of what has been widely known as possible: cyberattacks can shut down public utilities, deny wide populations services necessary for survival and escape precise attribution.

PURA Cybersecurity Action Plan at 5 et seq.

## [2014 Cybersecurity and Connecticut’s Public Utilities Report](http://www.governor.ct.gov/malloy/lib/malloy/2014.04.14_pura_cyber_report.pdfhttp:/www.governor.ct.gov/malloy/lib/malloy/2014.04.14_pura_cyber_report.pdf)

The [Cybersecurity and Connecticut’s Public Utilities Report](http://www.governor.ct.gov/malloy/lib/malloy/2014.04.14_pura_cyber_report.pdf) was [released on April 14, 2014](https://www.ct.gov/pura/cwp/view.asp?A=4144&Q=543340), having been prepared by the Public Utilities Regulatory Authority (PURA) at the direction of Governor Malloy and Connecticut’s General Assembly in response to the adoption of the state’s [2013 Comprehensive Energy Strategy for Connecticut](https://www.ct.gov/deep/lib/deep/energy/cep/2013_ces_final.pdfhttps:/www.ct.gov/deep/lib/deep/energy/cep/2013_ces_final.pdf). They directed the Public Utilities Regulatory Authority (PURA) to review the state's electricity, natural gas and major water companies and to assess the adequacy of their capabilities to deter interruption of service and to present to the Governor and General Assembly recommended actions to strengthen deterrence. In the 2013 Strategy the legislation directed PURA to prepare an unclassified cybersecurity review to assess Connecticut’s electric, natural gas and major water companies capabilities to deter cyber-related service interruptions and present recommended actions to strengthen deterrence.

The Report (at 6) noted that the cyber vulnerability of public utilities affects a large portion of Connecticut citizens, greater perhaps that the other “concentric circles of vulnerability” in Connecticut, which include manufacturing tied to national security, such as the production of aircraft engines, helicopters and submarines, as well as the state’s extensive insurance, financial management, retail banking, and health industries.

## [2013 Comprehensive Energy Strategy for Connecticut](https://www.ct.gov/deep/lib/deep/energy/cep/2013_ces_final.pdfhttps:/www.ct.gov/deep/lib/deep/energy/cep/2013_ces_final.pdf)

The [2013 Connecticut Comprehensive Energy Strategy](https://www.ct.gov/deep/lib/deep/energy/cep/2013_ces_final.pdfhttps:/www.ct.gov/deep/lib/deep/energy/cep/2013_ces_final.pdf) (2013 Energy Strategy), prepared by the Connecticut Department of Energy and Environmental Protection, and issued on February 19, 2013. The 2013 Energy Strategy was a report serving as a starting point toward defining regulatory guidance specifically for defensive cyber strategies. As chairman of PURA, Arthur House was directed to review the state's electricity, natural gas and major water companies and to assess the adequacy of their capabilities to deter interruption of service. Cybersecurity was noted, at 100, as requiring a “concerted effort will be required to develop a game plan to meet this standard of protection – and this Strategy makes improved cyber security a priority.” The report specifically called up PURA to conduct

a review of Connecticut‘s electricity, natural gas and major water companies to assess the adequacy of their capabilities to deter interruption of service. An unclassified report of such review together with recommended actions to strengthen deterrence should be presented to the Governor and General Assembly by September 1, 2013.

2013 Energy Strategy, at 111.

# Workforce Development for Cybersecurity talent gaps

Cybersecurity talent gaps exist across the country and this [Heat Map](https://www.cyberseek.org/heatmap.html) displays data illustrating that Connecticut has about 3,000 cyber security positions in need of employees, but there are no more than 300 students in the educational pipeline at this point. Just for example, the Hartford-West Hartford-East Hartford, CT metro area is in need of nearly 1,000 cyber security professionals, while the New Haven-Milford metro area needs to fill nearly 200 positions.

**Cybersecurity Educational Programs in Connecticut**

* <https://www.cyberdegrees.org/listings/connecticut/>
* [University of New Haven](http://wtnh.com/?s=university+of+new+haven), a private school, operates the UNH Cyber Forensics Research & Education Group / Lab (Est. 2013), <https://www.unhcfreg.com/>, which provides an online Master of Science in Investigations with a concentration in Forensic Computer Investigations. Completing the yearlong MS should prepare graduates to pass the Digital Forensics Certification Board (DFCB) and Certified Cyber Crimes Investigator (CCCI) as well as certifications covering money laundering and financial crimes. At the Tagliatela College of Engineering (TCoE), the UNHcFREG is charged with the mission of creating courses for two focus areas - namely Cyber Forensics Science and Cyber Security. *See* <https://www.unhcfreg.com/courses>
* Since 2012, the [Center for Hardware Assurance, Security and Engineering (CHASE Center)](https://chase.uconn.edu/) has been physically located in UConn’s new Information Technology Building. In that time, it’s won some major grants, including one from the U.S. Department of Defense worth $7.5 million to research security upgrades for nanoscale hardware. By garnering lucrative sponsorships from government agencies and corporations, CHASE provides embedded students with a chance to impress dozens of prospective employers.
* Given UConn’s reputation as a leader in hardware security research, the Storrs campus was a perfect location for the [Comcast Center of Excellence for Security Innovation (CSI)](http://www.csi.uconn.edu/) back in 2014. CSI now hosts the annual CyberSEED conference and hackathon for college cyber security teams around the country.
* In late 2016, Synchrony Financial announced the creation of the [Center of Excellence in Cybersecurity](http://today.uconn.edu/2016/10/uconn-establishes-synchrony-financial-center-excellence-cybersecurity/) at UConn. The Stamford-based company pledged to give $2.2 million over five years to fund fellowships and scholarships for graduate-level researchers. Synchrony sees this as an opportunity to breed and recruit fresh talent to its ranks.
* **Capital Community College, Hartford, Connecticut**, offers a [A.S. in Computer Networking: Cybersecurity Option](https://www.capitalcc.edu/academics/degrees/computer-networking-cybersecurity-option/) and a [Certificate in Cybersecurity](https://www.capitalcc.edu/academics/certificates/cybersecurity/). Many of the state’s community colleges and other private schools also offer concentrations in cybersecurity.
* **Charter Oak State College**, Connecticut’s online public college, provides online baccalaureate and certificate programs in cyber security.

# Connecticut Cybersecurity Resources

**Art House**

<https://portal.ct.gov/connecticut-cybersecurity-resource-page>

[Art House was appointed by Connecticut Gov. Dannel Malloy](https://www.securitymagazine.com/articles/87513-connecticut-names-states-first-chief-cybersecurity-risk-officer) in 2016 to be the state’s first [Chief Cyber Security Risk Officer](https://ctmirror.org/2016/10/12/arthur-house-to-leave-pura-oversee-cybersecurity-planning/) to be a leader for the state in increasing the state's cybersecurity safeguards protecting critical public and private infrastructure. [As the former chairman of PURA, House](https://inbound.kelsercorp.com/blog/why-connecticut-is-a-global-leader-in-cybersecurity) worked closely with public service companies regulated by the Authority and [Mark Raymond, the Chief Information Officer in Connecticut](http://www.hartfordbusiness.com/article/20110519/NEWS01/305199987/ct-hires-mark-raymond-as-cio) and the Connecticut Cyber Security Committee to develop the various cybersecurity documents referenced in this document to support enhanced cybersecurity techniques to protect the assets and reliability of the state’s electric, natural gas, and water utilities.

Two interviews with Art House, [Cyber Security Dispatch](https://cybersecuritydispatch.com/dispatch/2018/5/7/keeping-the-lights-on-an-interview-witharthur-house-chief-risk-officer-for-the-state-of-connecticut7) and [The State of Connecticut Cybersecurity](https://inbound.kelsercorp.com/blog/the-state-of-connecticut-cybersecurity-qa-with-arthur-house) present details on the work that House is performing in cybersecurity defenses on behalf of the state.

**Connecticut Cybersecurity Resources Page**

<https://portal.ct.gov/connecticut-cybersecurity-resource-page>

## Cyber Security Meetups & Communities in Connecticut

Several professional associations have planted chapters in the Constitution State. We highlight the most prominent dues-collecting organizations below as well as some free gatherings:

* [Connecticut ISSA](http://www.issa-ct.org/about-us): ISSA, which stands for Information Systems Security Association, is a professional organization that welcomes student members. If you join the Connecticut chapter in Danbury, you’ll get access to networking events and occasional presentations from outside speakers.
* [CT2600](http://ct2600.com/): Like 2600 groups across the country, the Newington-based version meets the first Friday of every month for discourse and demos on information security and hacking. Everyone is welcome.
* [Hartford Cyber Security Meetup/OWASP](https://www.meetup.com/Hartford-Cyber-Security-Meetup-OWASP/): The cyber security pros and proteges in the Hartford chapter of the Open Web Application Security Project (OWASP) meet infrequently for presentations and conversations with local industry experts.
* [ISACA Hartford Chapter](http://www.isaca.org/chapters6/hartford/Pages/default.aspx): ISACA, which used to be called the Information Systems Audit and Control Association, is another professional organization accepting student members. The Hartford chapter meets roughly once a month for seminars led by experts from the private and academic sectors.
* [(ISC)2 Southern Connecticut Chapter](http://www.isc2ct.org/): Paying Connecticuter members of the International Information Security Certification Consortium, or (ISC)2, meet quarterly in Shelton, where they discuss current trends and attacks and explore methods to respond to them.
* [BSidesCT](http://www.securitybsides.com/w/page/114611590/BSidesCT2017): BSides is a big annual event for the local cyber security community because it’s locally organized and executed, meaning you’ll find the experts next door instead of big-name keynote speakers. The daylong, low-cost event typically incorporates hour-long presentations alongside lightning talks and the occasional Capture the Flag competition.
* [Connecticut Risk Management Conference](http://risk.business.uconn.edu/risk-management-conference): The UConn School of Business puts on this annual conference in Stamford, which isn’t exclusively dedicated to cyber security but increasingly incorporates long sessions on cyber risk.
* [CyberSEED](http://www.csi.uconn.edu/cyberseed/): UConn’s Center of Excellence for Security Innovation has been putting on CyberSEED since 2014. CyberSEED’s main draw is the cyber security challenges for college teams in Capture the Flag, social engineering and secure coding. But the two-day conference also pulls in impressive keynote speakers (e.g., the tech consultants for Mr. Robot) and coordinates expert panels.
* [Hartford Tech-Security Conference](https://www.dataconnectors.com/event/hartford2019/): Although you can pay for access to sessions that provide continuing professional education credits, the main point of this free one-day event is to see what new products big companies have out. You’ll see this during sponsor presentations as well as at vendor booths.
* [North East Annual Cybersecurity Summit (NEACS)](http://neacs.org/): NEACS is an exclusive three-day event for business managers and executives to collaborate with tech experts. By joining conference organizers ISACA or (ISC)2, you can attend the workshops, listen to any of the tracked panel discussions, and network with business leaders.
* Cyber tips and resources can be accessed through the campaigns website at [**https://www.dhs.gov/stopthinkconnect#**](https://www.dhs.gov/stopthinkconnect)
* [**Tips for Organizations and Individuals to Protect Against Cyberattacks**](https://portal.ct.gov/-/media/Office-of-the-Governor/Connecticut-Cybersecurity-Resource-Page/DESPP-cybersecurity-safety-tips.docx?la=en)
* [**Sample Cyber Incident Response Plan Template**](https://portal.ct.gov/-/media/DAS/BEST/Security-Services/Incident-Response-Plan-template.doc?la=en)
* [**US Computer Emergency Response Team (US-CERT)**](https://www.us-cert.gov/ncas/tips)
* [**US Dept. of Homeland Security Stop-think-Connect Toolkit**](https://www.dhs.gov/stopthinkconnect-toolkit)
* [**Microsoft Safety and Security Center**](https://www.microsoft.com/en-us/safety/)
* [**Warning signs of malware infection**](https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/)
* [**SANS Tip of the Day**](https://www.sans.org/tip-of-the-day)
* [**TED Talks: Everyday Cybercrime and what you can do about it**](https://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it)
* [**FCC small business cybersecurity**](https://www.fcc.gov/general/cybersecurity-small-business)
* [**NIST Cybersecurity Framework**](https://www.nist.gov/news-events/events/2017/03/cybersecurity-framework-virtual-events)

## Resources in Case of an Attack

* The Internet Crime Complaint Center (IC3)
  + www.ic3.gov/default.aspx
* Identity Theft Resource Center
  + www.idtheftcenter.org
* Federal Trade Commission
  + www.identitytheft.gov
  + www.ftc.gov/complaint
* StopFraud.Gov
  + www.stopfraud.gov/victims.html
* U.S. Computer Emergency Readiness Team
  + www.us-cert.gov
* U.S. Department of Justice
  + [www.justice.gov/criminal/cybercrime](http://www.justice.gov/criminal/cybercrime)